

Final Proposal

by Hridoy Majumder

Submission date: 08-May-2026 06:44AM (UTC+0100)

Submission ID: 282722264

File name: 69767_Hridoy_Majumder_Final_Proposal_726821_616714534.docx (38.61K)

Word count: 3402

Character count: 20202

Research Methods and Professional Development (ACFA7004)

Evaluating the Forensic Recoverability of Browser Session Artifacts from Volatile Memory in Incident Response Scenarios

Submission to: Dr Seena Joseph
Module: Research Methods and Professional Development
Name: Hridoy Majumder
Department: Cyber security & Digital Forensics
ID: 2522065

University of Wales Trinity Saint David

Table of Content

Abstract.....	page (2)
Introduction.....	page (2-7)
Context & Background.....	page (2-3)
Research Problem.....	page (3-5)
Research Aim & Objective.....	page (5-6)
Significance of the Research.....	page (6-7)
Literature Review.....	page (7-8)
Research Design & Methodology.....	page (8-11)
Expected Outcomes.....	page (11)
Timeline.....	page (12)
References.....	page (13)

Evaluating the Forensic Recoverability of Browser Session Artifacts from Volatile Memory in Incident Response Scenarios

Abstract

Web browsers have changed into complicated application environments that handle authentication, encrypted communications, and interactions in the cloud. As a result, they have become one of the main sources of digital evidence in cybercrime investigations. Traditional forensic methods look at non-volatile storage, which is where things like browsing history, cookies, and cached files are kept. But modern Chromium-based browsers use advanced security features like encryption, sandboxing, and session-based authentication to limit how long important data can stay on disk.

This study examines the forensic recoverability of browser session artifacts retained in volatile memory (RAM). It looks into whether transient data like authentication tokens, session identifiers, and decrypted credentials can be safely pulled out during incident response situations. A regulated experimental approach is employed, incorporating simulated browsing activities, real-time memory acquisition, and post-mortem disk examination.

The research contrasts volatile and non-volatile artifacts employing evaluation criteria including completeness, integrity, and evidential relevance. The results should show that volatile memory holds unique and useful evidence that can't be found using traditional methods. This study enhances digital forensic methodologies and offers practical direction for incident response protocols.

1. Introduction

1.1 Context and Background

Cyber security has changed a lot over the years, and this has made the need for advanced digital forensics techniques that can deal with modern cyber threats much greater. As attackers use web-

based platforms more and more, web browsers have become an important part of forensic investigations. Browsers make it easy for users to do a lot of things, like log in, manage sessions, and send encrypted messages. This makes them a great source of evidence.

Modern browsers, especially those built on the Chromium architecture, use a multi-process model. This means that different processes are in charge of rendering, networking, and user interface tasks. This architecture makes security better by keeping processes separate, but it also breaks up data into different memory regions, which makes forensic analysis harder [3]. For example, session tokens and cookies could be stored in renderer processes, while  related to the network could be handled by different processes.

From a technical point of view, browser artifacts are kept in both permanent and temporary forms. SQLite databases in the file system usually store persistent artifacts like cookies and browsing history [1]. However, transient artifacts, like decrypted HTTPS content, JavaScript heap objects, and active session tokens, are kept in memory structures while the program is running [8].

Encryption makes it even harder to recover data forensically. Chromium-based browsers use operating system APIs like the Windows Data Protection API (DPAPI) to encrypt passwords that are saved [2]. These encrypted values may be stored on disk, but their decrypted versions are often only in RAM while the session is active. This makes getting memory a very important part of getting all the evidence back.

By looking at memory dumps, memory forensics can get this kind of unstable data. Tools like the Volatility Framework find artifacts in memory images by using techniques like signature scanning and structure carving [9]. But because browser memory structures are so complicated and dynamic allocation and garbage collection are used, it's hard to reliably get session-specific artifacts.

Even with these problems, volatile memory is still a useful source of forensic evidence, especially when systems are still running during an incident response. To improve forensic methods, it is important to know what kinds of browser artifacts can be found in memory and how useful they are as evidence.

1.2 Research Problem

The main problem this research tries to solve is that traditional disk-based forensic methods are becoming less useful for capturing transient browser session artifacts in modern computing environments. Traditional methods depend a lot on looking at non-volatile storage after the fact,

but changes in browser architectures and security systems have made it much harder for important forensic data to stay around.

Modern web browsers, especially those built on Chromium, use session-based authentication models and dynamic memory allocation. This means that sensitive information is only processed and stored during active sessions. Because of this, important artifacts like authentication tokens, session cookies, OAuth tokens, and Transport Layer Security (TLS) session keys may only be stored in volatile memory (RAM) and not written to disk in a way that can be recovered [8]. This poses a fundamental constraint for forensic investigations that depend exclusively on disk imaging.

From a technical point of view, these artifacts are stored in complicated memory structures, like heap allocations, stack frames, and shared memory segments. The browser and the operating system manage these structures on the fly. For instance, authentication tokens might be kept in the memory of the renderer process for a short time, while session data related to the network might be kept in separate network service processes. Because memory is often allocated and freed up, and garbage collection is used, this kind of data is very unstable and can be quickly overwritten when the session ends.

In addition, modern browsers have advanced anti-forensic and privacy-protecting features that make it even harder to recover evidence. Process isolation, sandboxing, and encrypted storage are all ways to keep sensitive data in persistent storage from being seen by others [5]. These mechanisms are necessary for keeping users' privacy safe, but they also make forensic analysis harder by making it harder to find recoverable artifacts.

Another important problem is that there aren't any standardized methods or specialized tools for getting browser-specific artifacts out of volatile memory. Volatility and other memory forensic frameworks are mainly made for looking at the structures of operating systems as a whole, not for looking at application-level data. As a result, investigators frequently utilize heuristic-based methodologies, which can result in inconsistent artifact recovery, incomplete reconstruction of session data, and possible evidential inaccuracies [9].

Moreover, there exists a paucity of empirical studies that compare the evidential value of volatile memory artifacts to those derived from non-volatile storage. It is uncertain whether the incorporation of memory forensics substantially improves the efficacy of digital investigations in the absence of comparative analysis. This lack of clarity makes it hard for incident response teams to decide whether to prioritize live memory acquisition when time is of the essence.

This research aims to tackle these challenges by methodically assessing the forensic recoverability, reliability, and evidential significance of browser session artifacts in volatile

memory, as well as their contribution to the advancement of contemporary digital forensic methodologies.

1.3 Research Aim and Objectives

Aim



To assess the forensic recoverability and evidential significance of browser session artifacts retrieved from volatile memory.

The main goal of this study is to carefully look at the forensic recoverability, reliability, and evidential significance of browser session artifacts taken from volatile memory (RAM) during incident response situations.

The study aims to ascertain whether volatile memory harbors unique, time-sensitive, and contextually rich forensic evidence that cannot be retrieved via conventional disk-based analysis. The research also seeks to evaluate how the incorporation of memory forensics can improve the comprehensiveness and precision of digital investigations.

From a technical standpoint, the study concentrates on elucidating the methods by which contemporary Chromium-based browsers handle session data within memory constructs, including process heaps, shared memory segments, and runtime buffers. The goal of the research is to find out if volatile memory can hold valuable artifacts like decrypted credentials, authentication tokens, and active session data, which are important for figuring out what users did during cyber incidents [8].

The ultimate goal goes beyond just recovering artifacts; it also includes improving methods, which will help create better and more complete forensic investigation strategies for modern computing environments.

4 Objectives

To reach the goal, the research will work toward the following specific goals:

1. To identify and classify browser session artifacts produced during active user interactions in Chromium-based environments, encompassing cookies, tokens, and runtime data structures.
2. To look at how modern browsers store session data across different processes (like renderer and network processes) and how this affects forensic recoverability [3].
3. To create and carry out controlled incident response scenarios that mimic real-world tasks like logging in, downloading files, and secure communications.
4. To get live memory during active sessions so that volatile artifacts are saved before they are lost when the system shuts down or the session ends.
5. To use forensic tools like the Volatility Framework to get browser artifacts from memory images and put them back together, using methods like memory scanning and structure reconstruction [9].
6. To get back artifacts from non-volatile storage, like SQLite databases and cache files, with tools like Autopsy and FTK Imager.
7. To do a comparative analysis of volatile and non-volatile artifacts using important forensic metrics like completeness, integrity, temporal accuracy, and evidential relevance.
8. To assess the forensic importance of volatile memory artifacts in facilitating incident response investigations, especially in instances of credential misuse or session hijacking.
9. To come up with useful suggestions for how to add memory forensics to regular investigative processes.

1.4 Significance of the Research

This study is very important for both academics and professionals in the field of digital forensics. From an academic standpoint, it fills a significant void in the current literature, as most studies concentrate on disk-based artifact recovery, largely neglecting the forensic capabilities of volatile memory in browser contexts.

In terms of memory forensics, the study adds to what we know, especially when it comes to application-level analysis. Prior studies have established that volatile memory can harbor

sensitive data, including credentials and encryption keys [8] [9]. However, there is a paucity of knowledge regarding the organization, storage, and retrieval of browser-specific artifacts within memory.

The research has direct effects on how incident response teams work in real life. In real-world situations, investigators often have to choose whether or not to do live memory acquisition because they don't have much time. This research delivers evidence-based insights regarding the significance of such actions, facilitating more informed decision-making.

The results may also help improve forensic tools and methods, especially those that work well with modern browser architectures. The research can help future innovations in forensic software design by pointing out the flaws in current methods.

Lastly, the study is important for society as a whole because better forensic skills can help with cybercrime investigations, court cases, and digital security practices.

2. Literature Review

Research in browser forensics has primarily concentrated on the retrieval and examination of artifacts preserved in non-volatile storage, especially those housed in structured databases like SQLite [1]. These artifacts, such as browsing history, cookies, cache files, and download records, keep a permanent record of what a user does. Many studies have shown that forensic tools can be used to get this kind of data, which lets investigators put together timelines and see how users interacted with each other. However, this method relies on the idea that important data is stored on disk, which is becoming harder to do with modern browser designs.

Recent research underscores the increasing intricacy of browser architectures and their ramifications for forensic analysis. Chand et al. [3] stress that modern browsers use a multi-process architecture, which means that different parts of the browser, like rendering engines, networking modules, and extensions, run in separate processes. This design makes the system more secure and stable, but it also spreads data across different memory areas, which makes it hard to use traditional methods to connect artifacts and figure out how users behave.

Forensic investigations have become even more difficult because of the addition of private browsing and incognito modes. Fernández-Fuentes et al. [4] show that even though these modes try to stop browsing data from being saved on disk, there may still be leftover artifacts in temporary files or memory. This indicates that volatile memory might function as an alternative source of evidence when persistent storage is deliberately reduced. But it's still not clear how reliable it is to recover these kinds of artifacts.

At the same time, research on anti-forensic techniques has looked into ways to hide or get rid of digital traces. Oh et al. [5] talk about how modern browsers use features like encrypted storage, safe memory handling, and automatic data deletion. All of these features make it harder to find

recoverable artifacts. These changes show a basic conflict between user privacy and forensic visibility, where better security may unintentionally make it harder to investigate.

Memory forensics research offers significant insights into the viability of volatile data as an evidentiary source. Ligh et al. [8] show that RAM can hold very private information, such as plaintext passwords, encryption keys, and application data structures. Case et al. [9] also stress the importance of live memory acquisition in incident response situations, where volatile data can give you real-time information about what is going on with the system. These studies provide the theoretical framework for the analysis of volatile memory in forensic investigations.

Nonetheless, in spite of these progressions, a considerable deficiency persists in the utilization of memory forensics pertaining to browser-specific artifacts. Current research predominantly emphasizes low-level operating system structures rather than application-level data, leading to a constrained comprehension of the representation of browser session artifacts in memory [10]. For instance, although it is established that authentication tokens and session cookies can reside in RAM, there is a paucity of empirical evidence concerning their recoverability, structure, or evidential reliability.

Additionally, contemporary research is deficient in a methodical comparison between volatile and non-volatile artifacts, especially within incident response contexts. It is challenging to evaluate the practical advantages of integrating memory forensics into conventional investigative workflows without such comparative analysis.

This research seeks to address this deficiency by delivering a comprehensive and comparative analysis of browser session artifacts in both volatile and non-volatile contexts. By doing this, it hopes to add to the current body of knowledge and help make digital forensic methods that are more complete and useful.

3. Research Design and Methodology

3.1 Research Design

This study employs a controlled experimental design alongside a simulation-based methodology, which is especially appropriate for digital forensic inquiries. The experimental design facilitates the methodical creation, collection, and analysis of browser artifacts in controlled conditions, guaranteeing repeatability and dependability.

The study adheres to a design science research framework, aiming not only to analyze existing phenomena but also to formulate and assess a structured forensic methodology. This framework is suitable as the research encompasses both artifact generation (via simulated browsing activities) and artifact assessment (through forensic analysis).

We will use a virtualized environment to mimic real-world computing situations. This includes

setting up a Windows 11 virtual machine that can run Chromium-based browsers. Virtualization has many benefits, such as the ability to control execution, easily copy systems, and take snapshots of system states at certain times.

The research design includes a comparative framework that compares artifacts found in volatile memory to those found in non-volatile storage. This comparison is necessary to figure out how memory forensics adds value.

From a technical point of view, the design takes the following things into account:

- Modern browsers use process-level isolation, which spreads data across different memory spaces.
- Dynamic memory allocation, which means that artifacts may be spread out over heap structures
- Temporal volatility, which means that data is only available during active sessions

By taking these things into account, the research design makes sure that forensic recoverability is fully tested.

3.2 Research Methods

The study utilizes a mixed-method approach, integrating quantitative and qualitative techniques to analyze forensic artifacts.

Experimental Method

A controlled experiment will take place in a virtual lab setting. We will simulate user activities to make browser artifacts that look real. Some of these activities are:

- Getting into web apps
- Getting to services that are protected by HTTPS
- Getting files to your computer
- Completing online forms

Each activity is meant to create certain types of session artifacts, like authentication tokens, cookies, and cached data.

Memory Acquisition

Magnet RAM Capture and other tools will be used to get live memory. This process takes a picture of the system's volatile memory while the browser session is still going on. When you get something is very important because it affects when you can use temporary artifacts.

Memory Analysis

We will use the Volatility Framework to look at the memory images that were taken. This means:

- Using process enumeration to find browser processes
- Scanning memory to find artefacts in memory regions
- Structure reconstruction to rebuild data structures like session tokens

These methods let you get both structured and unstructured data from memory [9].

Disk Analysis

We will use FTK Imager and Autopsy to get back disk-based artefacts. These tools let you get to browser databases, cache files, and system logs.

Data Analysis and Evaluation

We will use the following metrics to evaluate artefacts:

- Completeness: how much data was recovered
- Integrity means being correct and consistent.
- Time accuracy means that the information matches the user's activity timeline.
- Evidential relevance – helpfulness in an investigation

After that, a comparative analysis will be done to find the differences between volatile and non-volatile artefacts..

3.3 Data Collection

- Simulated user activity
- Controlled environment
- Virtual machine

3.4 Tools

- Volatility Framework
 - FTK Imager
 - Autopsy
 - RAM Capture tools
-

4. Expected Outcomes

It is expected that volatile memory will hold unique artefacts that are not found on disc. This might make forensic work better.

The anticipated results of this research go beyond just recovering artefacts; they also aim to offer both technical insights and practical contributions to the field of digital forensics.

First, volatile memory analysis is expected to show a wider and more detailed set of browser session artefacts than traditional methods that use discs. These may consist of decrypted credentials, active session tokens, and in-memory representations of web content, which are generally inaccessible in persistent storage [8]. The existence of such artefacts would underscore the paramount significance of memory acquisition in the collection of time-sensitive evidence. Secondly, the study is anticipated to underscore notable disparities in artefact completeness and temporal precision between volatile and non-volatile sources. Disk-based artefacts may give us information about the past, but volatile memory is probably a better way to see what users are doing right now. This difference is very important when responding to an incident, when it's important to know what happened in what order.

Finding flaws in current forensic tools and methods is another expected result. For instance, problems with process isolation, encrypted data, and broken memory structures could make it harder to recover artefacts. By writing down these limits, the research can help make forensic methods better.

From a practical standpoint, the results are anticipated to offer explicit guidance for incident response protocols, especially concerning the timing and methodology of memory acquisition. This could include rules for how to priorities capturing volatile memory in real-time investigations.

Lastly, the study will probably help the field of digital forensics as a whole by linking memory forensics and browser artefact analysis. This integration can make forensic investigations more effective overall and help create more complete analytical frameworks.

5. TIMELINE

Task / Phase	May 2026	Jun 2026	Jul 2026	Aug 2026	Sep 2026	Oct 2026	Nov 2026	Dec 2026
Literature Review								
Research Design & Planning								
Lab Setup & Tool Configuration								
Data Collection (Simulation)								
Memory & Disk Acquisition								
Data Analysis								
Results Evaluation								
Report Writing								
Final Editing & Submission								

The research project will take place from May to December 2026, which is eight months long. The timeline is set up so that the steps go in a logical order, starting with the literature review and experimental setup, then moving on to data collection, analysis, and finally writing the report. In the early stages, the focus is on understanding the theory and getting the environment ready. In the later stages, the focus is on doing the experiment and judging it critically.

6. REFERENCES

- [1] Majeti et al., 2023.
 - [2] Raza et al., 2024.
 - [3] Chand et al., 2025.
 - [4] Fernández-Fuentes et al., 2025.
 - [5] Oh et al., 2022.
 - [6] Rzaeva et al., 2026.
 - [7] Ali et al., 2022.
 - [8] Ligh et al., 2021.
 - [9] Case et al., 2021.
 - [10] Quick et al., 2022.
-

Final Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

40/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4



Comment 1

should be started with [1]



Comment 2

Too long research problem statement. Make it shorter and support it with the literature,

PAGE 5

PAGE 6



Comment 3

Revisit the aim and state only the overarching aim of the study

PAGE 7



Comment 4

Too many objectives.. reduce to 4-5 SMART objectives

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

GRADING FORM: ACFA7004 PROPOSAL MAY 2026

HRIDOY MAJUMDER**40****ENGAGEMENT WITH LIT.SKILL [30]**

Structure and Organization of the literature review [8 Marks] Critical Engagement with Literature [10 Marks] Relevance and Positioning of Your Study [7 Marks] Recent and Relevant in-text citations and reference list [5 Marks]



The literature is presented in a very basic narrative form.

The review is largely descriptive with limited critical analysis. None of the references provided can be verified, as they are not sufficiently detailed. This raises a major concern regarding the quality and reliability of the sources. Please ensure to use the reliable sources and cite and reference them correctly as per the requirements.

10**KNOWLEDGE & UNDERSTANDING [20]**

Brief overview and current developments in the proposed research area [10 Marks] Research problem statement [7 Marks] Significance of the study [3 Marks]



The proposal demonstrates a basic understanding of the topic; however, explanations are often general and lack strong academic support from reliable sources.

The proposed research problem is conceptually

8

appropriate; however, it is not clearly stated and is not adequately supported by the literature.
The significance is broadly stated.

COGNITIVE & INTELLECTUAL [10]

Clearly state the aim of the research based on the identified research problem [5] Break down the research aim into smaller, measurable, and achievable steps [5]



The aim is relevant, but it needs to be rephrased; it is very long and lacks clarity. State the overarching aim of the study.

The objectives are poorly structured and largely task-based, focusing on procedural steps (e.g., using tools, collecting data) rather than clear research outcomes.

Please clearly state 4-5 SMART objectives

4

PRACTICAL APPLICATION [25]

*Research Design (Explanation of the overall research approach) [7]
Research methods [10] - a detailed explanation about the research methods to achieve the research objectives Research materials [8] - in terms of Software and hardware*



The design is mentioned (experiment/simulation).
No justification provided.

The research methodology needs to be improved.
it is not based on the standard research approach.
Understand the research process and state clearly how each research objective will be achieved.

10

TRANSFERABLE SKILLS [15]

Project planning and resource management [5 Marks] Description of the project's potential impact and limitations [5 Marks] - Expected outcome Presentation style [5 Marks]



The timeline provided needs to be revisited. The given dates are not realistic.

Expected outcomes are very generic.

The writing is not at the expected Master's level, as it includes informal phrasing, repetition, and lacks clarity.