

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

NAME: HRIDOY MAJUMDER

ID: 2522065

MSC CYBERSECURITY & DIGITAL FORENSICS

UWTSD

MODULE; RESEARCH METHOD AND PROFESSIONAL DEVELOPMENT

Research Context / Background

- ❖ Web browsers are central to modern cybercrime investigations
- ❖ Store authentication tokens, session IDs, credentials
- ❖ Chromium-based browsers use encryption & sandboxing
- ❖ Traditional forensics focuses on disk-based artifacts
- ❖ Volatile memory may contain critical session data



Literature Review

- ❖ Existing studies focus on:
 - Browsing history
 - Cookies & cache
 - SQLite databases
- ❖ Emphasis on post-mortem disk analysis
- ❖ Limited focus on volatile memory
- ❖ Minimal comparison between RAM and disk artifacts



Research Gap

- ❖ Critical session artifacts may exist only in RAM
- ❖ Limited empirical research on:
 - Session tokens in memory
 - Decrypted credentials in RAM
 - Live incident response acquisition

Research Gap



- ❖ No structured comparison of volatile versus non-volatile artifacts
- ❖ Gap in practical forensic procedures

Research Problem

- ❖ Modern browsers use:
 - Encryption
 - Session-based authentication
 - Multi-process architecture
- ❖ Disk analysis may miss key evidence
- ❖ Lack of clear guidance for live incident response
- ❖ Uncertainty about evidential value of RAM artifacts





Research Aim

❖ To evaluate the forensic recoverability and evidential value of browser session artifacts extracted from volatile memory during incident response scenarios.

Research Problem

- ❖ Identify browser session artifacts during active use
- ❖ Simulate incident response scenarios
- ❖ Acquire live memory images
- ❖ Extract and analyse RAM-based artifacts
- ❖ Compare with disk-based artifacts
- ❖ Evaluate evidential reliability



Research Methodology

❖ Experimental lab-based design

❖ Environment:

- Windows 11
- Google Chrome & Microsoft Edge

❖ Tools:

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

❖ Controlled browsing simulations

❖ Comparative artifact analysis

Project Planning & Resources

❖ **Timeline (6 Months):**

- Literature Review – Month 1
 - Lab Setup – Month 2
- Data Collection – Month 3
 - Analysis – Month 4
 - Writing – Month 5–6

Project Planning & Resources

❖ **Resources Required:**

- Virtual lab environment
- Forensic software tools
 - Test accounts

Project Impact & Limitations



❖ **Impact:**

- Improves live forensic practices
- Supports incident response investigations
- Contributes to browser forensics research

Project Impact & Limitations



❖ Limitations:

- Lab-based controlled environment
- Limited to Chromium browsers
- Time-bound MSc scope

References

Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques

Rishal Ravikesh Chand¹ · Neeraj Anand Sharma¹ · Muhammad Ashad Kabir²

Received: 28 October 2024 / Accepted: 22 March 2025 Published: 5 April 2025

© The Author(s) 2025

Digital Forensic Advanced Evidence Collection and Analysis of Web Browser Activity

K.V.P.S Ganesh Majeti^{1,*}, Y.V.L Sai Sundar¹, Sai Shanmukh Ulich¹, Sachi Nandan Mohanty¹, Sudha

SV

Received on 15 February 2023, accepted on 20 April 2023, published on 29 June 2023

References

An Intelligent Browser History Forensics Method for Automated Analysis of Web Activity Logs, Credentials, and User Behavioral Profiles

Leila Rzayeva 1,2,* , Aliya Zhetpisbayeva 1,* , Alisher Batkuldin 1 , Nursultan Nyssanov 1 , Alissa Ryzhova 1 and Faisal Saeed

Received: 28 November 2025 Revised: 5 January 2026 Accepted: 10 January 2026 Published: 16 January 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Digital forensic analysis of the private mode of browsers on Android ☆

Xosé Fernández-Fuentes *, Tomás F. Pena, José C. Cabaleiro

Centro Singular de Investigación en Tecnoloxías Intelixentes (CiTIUS), Departamento de Electrónica e Computación, Universidade de Santiago de Compostela, 15782 Santiago de Compostela, Spain

Received: 28 November 2024 Accepted: 9 January 2025 Published: 16 January 2025

References

Forensic analysis of web browsers lifecycle: A case study

Ahmed Raza ^a, Mehdi Hussain ^a, Hasan Tahir ^a, Muhammad Zeeshan ^a, Muhammad Adil Raja ^{b,c},

Ki-Hyun Jung ^{d,*}

^a *School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan*

^b *Regulated Software Research Center (RSRC), Dundalk Institute of Technology (DkIT), Dundalk A91 K584, Ireland*

^c *The Irish Software Research Centre, Lero, University of Limerick, Limerick, V94 T9PX, Ireland*

^d *Department of Software Convergence, Andong National University, 1375 Gyeongdong-ro, Andong-si, Gyeongbuk 36729, Republic of Korea*