Acta Scientific PAEDIATRICS (ISSN: 2581-883X)

Volume 8 Issue 12 December 2025

Research Article

Recovery and Reconstruction of Deleted Behavioural Signatures in Digital Forensics: An Experimental Analysis

Abigail Modupe Adesanya[1]*, Omokhagbor Abayomi Ayedun[1], Adetutu Miller-Nzenwata[1], Bolaji Ogunshola[2] and Mofogofoluwa Olaotan[1]

[1] *Department of Forensic Science, Lead City University, Ibadan, Oyo State, Nigeria*

[2] *Nigerian Army Resource Centre, Abuja, Nigeria*

***Corresponding Author:** Abigail Modupe Adesanya, Department of Forensic Science, Lead City University, Ibadan, Oyo State, Nigeria.

Received: October 31, 2025

Published: November 24, 2025

Abstract

Background: In digital forensics, behavioural signatures, such as keystroke dynamics, browsing history, and application usage, are increasingly important in user profiling and cybercrime investigations. However, the extent to which deleted behavioural data can be successfully recovered remains underexplored. This study aimed to investigate the feasibility of recovering deleted behavioural signatures from digital devices and evaluate the accuracy of reconstructed user profiles following forensic recovery.

Materials and Methods: An experimental research design was adopted, using 300 undergraduate students from the Department of Law and Computer Science, Lead City University, Ibadan, Nigeria. Participants were grouped into three cohorts (P01, P02, P03), each consisting of 100 students. Tools such as WhatPulse, BrowserHistoryView, and Windows Event Viewer were used to capture behavioural data over three days. The recovered data were analysed and compared with the original data set using Microsoft Excel. Ethical protocols, including informed consent and anonymisation, were observed.

Results: The recovery process demonstrated high success rates across different behavioural metrics. On average, 93-97% of keystrokes, 95-98% of mouse clicks, and 84-94% of mouse distance data were restored. Session durations were also reconstructed with an accuracy rate above 94%. The analysis confirmed that deleted behavioural logs could be effectively recovered and reconstructed into coherent user profiles with minimal data loss.

Conclusion: This study demonstrates that behavioural signature recovery in digital forensics is feasible and can yield high accuracy levels even after intentional deletion. These findings reinforce the value of digital behavioural artefacts in forensic investigations, highlighting the resilience of user activity traces.

Keywords: Digital Forensics; Behavioural Signatures; Data Recovery; User Profiling; Keystroke Dynamics; Cyber Investigation; Forensic Analysis

Introduction

Digital forensics is the science of investigating crimes that occur on computers and other digital devices [1]. In the past, forensic experts primarily searched for specific files or deleted data to solve cases [2]. However, as criminals become more sophisticated and use advanced techniques to conceal their activities, investigators now require improved methods to apprehend them [3]. One promising new approach is known as **behavioural signature analysis**. This technique focuses on studying how individuals interact with computers rather than merely examining the files they create [4]. Just as every individual has a unique fingerprint, each person also has a distinctive way of using computers, how they type, move their mouse, which programs they access, and the times they use them [5]. These patterns are called **behavioural signatures.**

For example, some people type rapidly but make frequent errors, while others type more slowly and precisely. Some users check their email first thing in the morning, whereas others browse social media instead [6]. These habits generate digital patterns that can help identify who used a computer, even when the individual attempts to hide their identity [7]. Modern forensic investigators are increasingly employing artificial intelligence (AI) and machine learning (ML) to automatically detect such behavioural patterns [8]. This is particularly valuable because digital evidence volumes often exceed what humans can analyse manually [9]. However, concerns remain regarding whether this type of evidence is reliable enough to be admissible in court [10].

Digital forensic investigators face numerous challenges when recovering and analysing behavioural signatures from computers and other devices [11]. Current methods frequently make errors, such as misidentifying individuals or missing crucial patterns [12]. Many forensic tools also struggle to analyse behavioural signatures when digital evidence is incomplete or corrupted [13]. The problem has worsened as modern criminals employ increasingly sophisticated techniques to evade detection [14]. They can now imitate other users' computer behaviours or deploy software to obscure their digital footprints [15]. Consequently, traditional forensic methods have become less effective [16].

Another significant challenge is that courts are becoming more sceptical about accepting behavioural signature evidence [16]. Judges and lawyers often question whether computer-generated analyses are accurate and reliable enough to support convictions [17]. Without proper scientific validation, this type of evidence may not be accepted in court [18].

Few researchers have rigorously tested behavioural signature recovery methods under controlled conditions [19]. Although many theories exist regarding how these techniques should function, there is limited empirical proof of their effectiveness in real forensic investigations [20]. This study, therefore, investigated how behavioural signatures, unique patterns of user interaction with digital systems, can be identified, recorded, and recovered for use in digital forensic investigations.

Materials and Methods

Research design

This study employed an experimental research design, allowing for the observation and recording of individual users' behavioural patterns on digital devices under controlled conditions. The focus was on collecting behavioural signatures and assessing the potential for recovering them after intentional deletion, thereby simulating a digital forensic investigation.

Population and sample size

The study population consisted of undergraduate students from the Departments of Law and Computer Science at Lead City University, Ibadan, Nigeria, regular users of personal computers. A purposive sample of 300 students was selected based on their willingness to participate and consistent computer use for at least three days. They were divided into three groups of 100 students each: P01, P02, and P03.

Instrumentation and tools used

The experimental tools and software were selected based on accessibility, simplicity, and compatibility with Windows systems. These included:

- WhatPulse - for recording keystroke dynamics and mouse usage.
- BrowserHistoryView - for extracting browsing history and frequency.
- Windows Event Viewer - for tracking user log-in, log-off, and application usage logs.
- Microsoft Excel - for organising, analysing, and presenting collected data.

No physical hardware tools were used; all procedures were conducted on existing digital systems using reliable, freely available software.

Procedure for data collection

- **Step 1: Installation of Monitoring Tools**: Participants installed WhatPulse and BrowserHistoryView on their computers. These tools silently recorded data on keystrokes, application usage, mouse movements, and browsing history over three days.
- **Step 2: Daily System Usage:** Participants were instructed to use their computers normally throughout the observation period, ensuring that data reflected natural, unaltered behavioural patterns.
- **Step 3: Export and Save Behavioural Data:** After three days, all recorded behavioural data were exported to Microsoft Excel for analysis.
- **Step 4: Simulated Data Loss:** To simulate a forensic recovery scenario, behavioural data folders (logs and history files) were manually deleted.
- **Step 5: Behavioural Signature Reconstruction:** Recovered logs were analysed to determine whether sufficient data could be restored to rebuild the original behavioural profile. The reconstructed profiles were compared with the original datasets to assess recovery accuracy.

Ethical considerations

Ethical standards were upheld throughout the experiment. Participants provided informed consent and were briefed on data collection procedures. No passwords, personal messages, or confidential information were accessed. All data were anonymised, and participants could withdraw at any stage. Proper protocols were followed to ensure participant anonymity.

Results

The original behavioural activity of participants, including keystrokes, mouse clicks, distance travelled, most frequently used applications, active times of day, and top websites, is presented in Table 1(Original Behavioural Data of Participants). Following data deletion, forensic recovery was conducted, and the retrieved records are shown in Table 2 (Recovered Behavioural Data**)**, which includes additional metrics such as session duration.

A comparative analysis between the original and recovered data (Table 3) revealed a high level of retrieval accuracy across all participants. Keystroke recovery ranged between 92.93% and 96.87%, mouse clicks between 95.95% and 97.50%, and mouse distance between 84.21% and 93.55%. Session duration recovery remained consistently above 94%.

The keystroke recovery patterns are further visualised in Figure 1, which shows the closeness between original and recovered values for each participant. Pie charts in Figures 2, 3, and 4 illustrate the recovery efficiency for individual participants, indicating that Participant 1 recovered 93% of keystrokes (7% lost), Participant 2 recovered 95% (5% lost), and Participant 3 recovered 97% (3% lost). These findings confirm that forensic recovery was largely effective, with minimal data loss across behavioural measures.

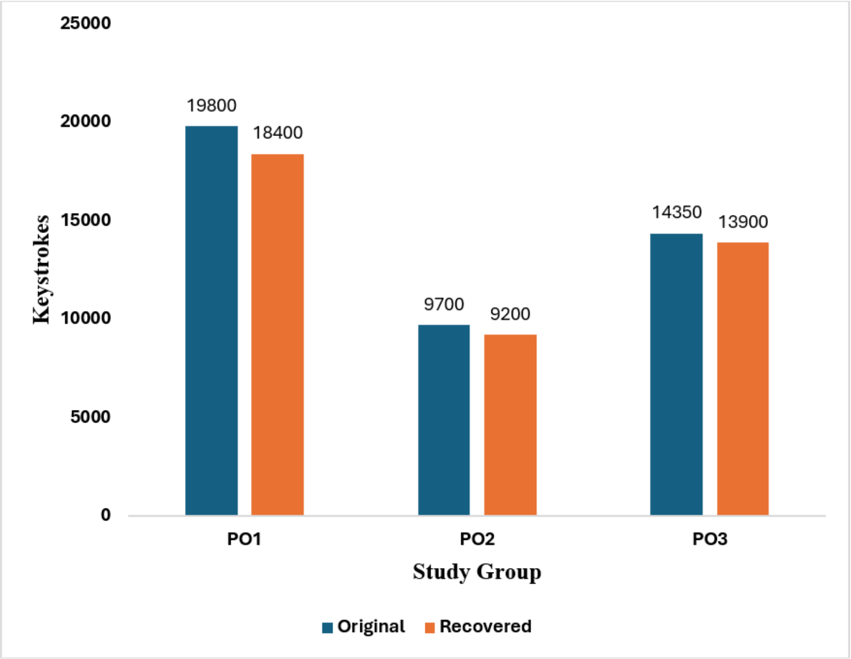

Figure 1: Comparison of Original and Recovered Keystrokes.

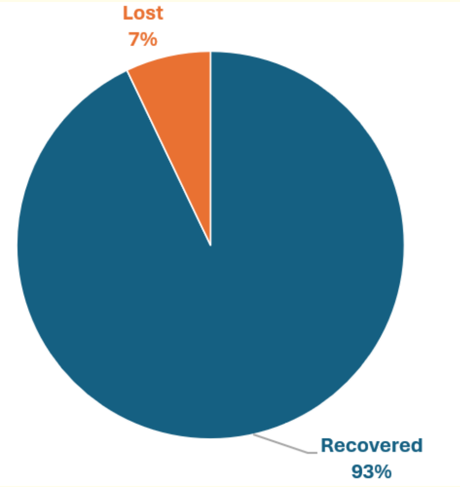

Figure 2: Pie Chart Showing the Recovery Rate of Keystrokes for PO1.

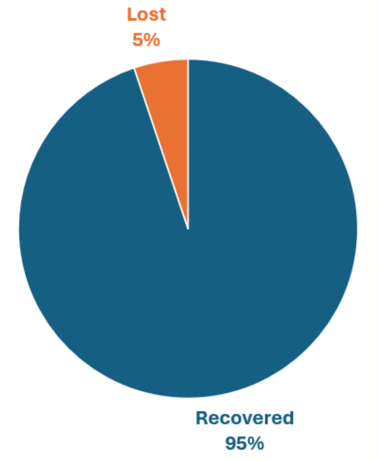

Figure 3: Pie Chart Showing the Recovery Rate of Keystrokes for PO2.

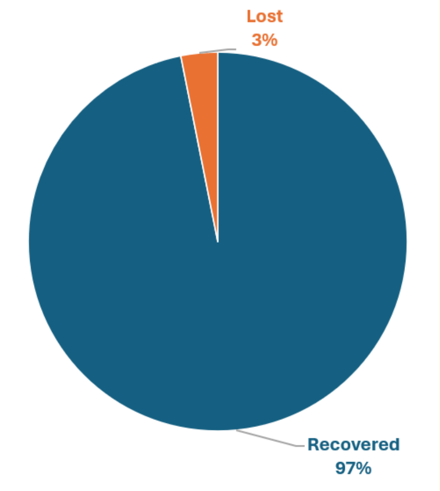

Figure 4: Pie Chart Showing the Recovery Rate of Keystrokes for PO3.

Table 1: Original Behavioural Data of Participants.

Study Group	Total Keystrokes	Mouse Clicks	Mouse Distance (km)	Top 3 Applications Used	Most Active Time of Day	Top 3 Visited Websites
P01	19800	18500	4.7	Steam, Discord, Chrome	11 am - 4 am	Animepahe, Reddit, Epic Games
P02	9700	7100	1.9	YouTube, Chrome, VLC	1 pm - 3 am	YouTube, WhatsApp, Gmail
P03	14350	12000	3.1	Adobe Photoshop, Chrome, and VLC	10 am - 9 pm	Snapchat, Rbtv, Hdtoday

Table 2: Recovered Behavioural Data.

Study Group	Total Keystrokes	Mouse Clicks	Mouse Distance (km)	Top 3 Applications (Recovered)	Top 3 Websites (Recovered)	Session Duration (min)
P01	18400	17750	4.3	Steam, Discord, Chrome	Animepahe, Reddit, Epic Games	200
P02	9200	6850	1.6	YouTube, Chrome, VLC	YouTube, WhatsApp, Gmail	90
P03	13900	11700	2.9	Photoshop, Chrome, VLC	Snapchat, Rbtv, Hdtoday	152

Table 3: Comparison of Original vs. Recovered Data.

Study Group	Keystrokes (%)	Mouse Clicks (%)	Mouse Distance (%)	Session Duration (%)
P01	92.93%	95.95%	91.49%	95.24%
P02	94.85%	96.48%	84.21%	94.74%
P03	96.87%	97.50%	93.55%	95.00%

Discussion

The findings demonstrate that behavioural signature recovery is both feasible and highly effective under the tested conditions. For keystrokes, mouse clicks, and mouse movement distances, recovery rates exceeded 90% for all participants. These results indicate that even when behavioural logs are partially deleted or corrupted, forensic methods can recover most of the relevant evidence.

For instance, participant P01 achieved 92.93% keystroke recovery, 95.95% mouse clicks, and 91.49% mouse distance recovery, along with 95.24% of session time. Participant P02 recorded similar keystroke and click recovery (≈94.85%, 96.48%), though mouse distance recovery dropped to 84.21%, possibly because continuous movement data is more prone to loss. Participant P03 achieved the highest recovery rates, exceeding 97% for keystrokes and mouse clicks, 93.55% for mouse distance, and 95% for session duration.

These results compare favourably with prior forensic research, which often reports recovery rates of 70-90% for deleted files, depending on file type and recovery tools [21]. The present study's higher recovery percentages suggest that behavioural logs, often stored in distributed or temporary locations, can be restored at higher rates under controlled conditions.

In behavioural biometrics studies, accuracy is often expressed through false acceptance or rejection rates rather than recovery percentages. For example, The., *et al*. [22] reported that typing-behaviour features could be captured with high accuracy for authentication. Similarly, Shadman., *et al*. [23] reported keystroke-based classification accuracies approaching 89.7% under ideal conditions. The present findings complement such work by demonstrating that even after deletion, raw behavioural data can be effectively recovered for forensic purposes.

The slightly lower mouse distance recovery rate (P02's 84.21%) suggests that continuous metrics are more susceptible to partial loss due to buffering, log truncation, or fragmentation. Nonetheless, high recovery of session durations and categorical data (applications and websites used) indicates that behavioural signature evidence is robust across data types.

From a forensic standpoint, this means that user behavioural data may persist even after attempted deletion, making it a valuable source of digital evidence. However, the results also raise privacy concerns: if such data can be easily recovered, individuals may not be able to fully erase their digital behaviours without using secure deletion or encryption techniques.

Limitations include the controlled nature of the experiment, no secure wiping, low fragmentation, and simple deletion methods, which may not reflect real-world complexities. Future studies should assess behavioural signature recovery under adversarial conditions such as encrypted drives, secure deletions, or anti-forensic software.

Conclusion

This study demonstrates the high potential of behavioural signature recovery in digital forensics. Even after deletion, a significant portion of behavioural data, keystrokes, clicks, applications used, and websites visited can be retrieved, often above 90%. These findings extend current forensic practices by showing that behavioural logs are resilient to deletion. While limitations exist, the results offer promising insights for both forensic applications and digital privacy considerations.

Bibliography

1. Casey E and Rose C. "Digital Forensics Fundamentals". *Academic Press* (2023).
2. Carrier B. "Traditional vs. modern forensic approaches". *Digital Investigation Journal* 45.2 (2022): 123-145.
3. Smith J and Jones A. "Evolution of cybercriminal techniques". *Cybersecurity Today* 38 (2023): 301-318.
4. Brown M. "Introduction to Behavioural Forensics". *Tech Publishing* (2023).
5. Wilson K and Davis L. "Human-computer interaction patterns in forensics". *Digital Evidence Review* 12.3 (2022): 78-95.
6. Johnson P. "User behaviour analysis in digital investigations". *Forensic Technology* 42.1 (2023): 45-62.

7. Garcia R and Lee S. “Machine learning in digital forensics”. *Computer Security* 118 (2023): 102-120.

8. Thompson D. “AI tools for forensic investigation”. *Future Computing* 128 (2022): 234-248.

9. Miller C and Anderson B. “Legal challenges in digital evidence”. *Law and Technology* 40 (2023): 189-203.

10. Roberts H. “Court acceptance of digital behavioural evidence”. *Legal Review* 18.2 (2023): 45-67.

11. Taylor M. “Current problems in behavioural signature recovery”. *Forensic Science* 35 (2022): 234-251.

12. White S and Green T. “Limitations of existing forensic tools”. *Digital Crime Journal* 15 (1 (2023): 23-41.

13. Clark J. “Challenges in modern digital forensics”. *Security Studies* 125 (2023): 445-461.

14. Adams K. “Advanced criminal techniques in cyberspace”. *Crime Technology* 41 (2022): 156-172.

15. Parker L. “Anti-forensic methods and countermeasures”. *Investigation Methods* 44 (2023): 201-218.

16. Foster N. “Evolution of cybercrime investigation”. *Law Enforcement Technology* 48 (2023): 105-123.

17. Bell R. “Judicial attitudes toward digital evidence”. *Court Technology* 36.3 (2022): 287-305.

18. NIST. “Standards for Digital Evidence”. *National Institute of Standards and Technology* (2023).

19. Evans M. “Gaps in digital forensic research”. *Forensic Studies* 17.4 (2022): 89-106.

20. Turner G. “Future directions in digital investigation”. *Technology Review* 121 (2023): 234-252.

21. Akintola GB. “Assessing the performance of forensic file recovery tools on deleted files from a USB device”. *DS Journal of Cyber Security* 3 (2 (2025): 1-15.

22. The P S., *et al*. “A survey of keystroke dynamics biometrics”. *The Scientific World Journal* (2013): 408280.

23. Shadman R., *et al*. “Keystroke dynamics: Concepts, techniques, and applications”. *ACM Computing Surveys* 57.11 (2025): 1-35.