UDC: 004.056.53:004.738.5

Huzaifa Sadi Yakasai; Dr. Fakhrun Jamal; Bello Musa Bello; Tijjani Adam Ahmad
Scientific supervisor: Dr. Fakhrun Jamal, Assistant professor at cse department mmu mullana Haryana
Shobhit University, India

BROWSER-BASED CLOUD STORAGE FORENSICS ON GOOGLE DRIVE ARTIFACTS IN FIREFOX

Abstract*. Cloud storage services are widely used globally, the users of the services are accessing the services using different devices from different locations, amongst which they used the services unethically like breaching someone's privacy and unauthorised access to an individual's or organization's data. But after the interactions with the services, there were some footprint of the suspects that can be found, which leaves some digital artifacts accessible through web browsers. This research focuses on gathering and analyzing forensic evidence from Firefox's SQLite database, targeting the user's interactions with Google Drive. By using 'places.sqlite' [1], [2]. We extracted the user's browsing history, metadata, and timestamps and convert it into human readable form. This analysis will help digital forensics professionals to understand the persistence of browser-based artifacts in forensic investigations and students for guidance on the steps for retrieving browser artifacts [3][4].*

Keywords: *cloud storage, digital forensics, browser forensics, Google Drive, Firefox.*

Хузаіфа Саді Яксаї; Д-р Фахрун Джамал; Белло Муса Белло; Тіджані Адам Ахмад
Науковий керівник: Д-р Фахрун Джамал, асистент-професор, Університет Махаріші Маркандешвара (MMU) у Муллані, штат Хар'яна, Індія
Університет Шобіт, Індія

БРАУЗЕРНА ФОРЕНЗІКА ХМАРНОГО СХОВИЩА GOOGLE DRIVE: ДОСЛІДЖЕННЯ АРТЕФАКТІВ У FIREFOX

1.0 Introduction

The continuous adoption and reliance on cloud-based services such as OneDrive, Google Drive, and Dropbox have had an impact on revolutionizing how the users store and access their information. However, with all this advancement in technology, it comes with some challenges, which include identifying, preserving, and analyzing digital evidence in these environments. When a user accesses the service on a device, it is possible to analyze browser artifacts and footprints that can provide valuable forensic evidence regarding his cloud interactions [5], [6].

This research is aimed at providing a beginner-friendly methodology, especially for students in the field of cybersecurity and digital forensics, by only focusing on browser-based digital forensic techniques. I perform this practical forensic investigation on a system that has Linux Mint OS with the following specifications: Intel Celeron N4020, 4GB RAM, and targeting Google Drive activity conducted by using the Firefox browser [7].

Cyber forensics is a discipline that focuses on identifying and mining digital evidence, analyzing cyber events and incidents, and playing a vital role in aiding legal authorities for the prosecution of culprits or cybercriminals and proving the innocence of innocent personnel.

This is the process of extracting, examining, analyzing, and reporting evidence data from digital devices (computers, smartphones, IoT devices), storage devices, and networks for legal proceedings such as civil cases or criminal investigations [7].

Cloud computing is a virtual data storage technique that saves a voluminous amount of data, which can be accessed remotely from different digital devices, which revolutionized the manual storage process. There are different storage providers that provide services of cloud computing, which

comprise collecting and storing of users' data with ultimate security and availability of the data. Users can retrieve their data from different locations and on different devices for individual and enterprise accounts. Cloud storage providers include Google Drive, Amazon, iCloud, OneDrive, and many more [8][9].

A web browser is a user application that enables a user to locate, display, and access web page contents through the internet. The most popular web browsers include Google Chrome, Mozilla Firefox, and Internet Explorer. Finding evidence and footprints in browsing history plays a crucial component of digital forensic investigation [10].

2.0 Related Work

Cloud forensics is a trending subfield in digital forensics. It comprises the identification, collection, preservation, examination, and analysis of digital evidence stored in cloud environments. The traditional drawbacks of cloud forensics include data volatility, jurisdiction, and multi-tenancy. Browser-based forensics is a subset that relies on customer-side analysis.

A lot of past research on web browser forensics has specific structural methods for certain log files. Mahajan et al. proved that web browsers are retaining remnants and artifacts even after the deletion attempts by the user [1]. Quick and Choo (2013) [9] and Daryabar et al. (2017) have examined the cloud forensics on different platforms; they highlight the importance of some tools in SQLite databases like cookies.sqlite and places.sqlite. And the Firefox browser plays the vital role of storing extensive logs in these databases, which makes it a valuable tool in conducting forensic analysis [10]. Martini and Choo (2012) and Jones (2003) explained the format of the index.dat file and the process of retrieving deleted records from Internet Explorer. He introduces a tool (pasco) for analysis of the index.dat file [11]. Fernandez-Fuentes et al. explained the impact on browsing modes, specifically private modes in Google Chrome and Mozilla Firefox across different Linux environments, by using certain forensic tools such as FTK Imager for creating forensic images, Autopsy for file system analysis, and other forensic tools for analyzing browser artifacts [2].

However, the related works still lack some practical processes and methodologies to extract and make the analysis based on the results from open-source tools, specifically browser-based in a Linux environment.

This research is aligned with the study of Singh et al. [12], who recommend using lightweight computer systems with Linux OS and using some of the open-source tools like Autopsy for the academic and hands-on practicals of forensic investigations, and the research also aims to investigate the forensic traces and footprints left behind using browser-based interaction with cloud storage (specifically Google Drive) using the Firefox browser on a Linux-based operating system (Mint) environment [11].

Research Question

How can forensic investigators and experts interpret and extract browser-based artifacts using SQLite to reconstruct a user activity on a cloud storage service like Google Drive in a Linux environment? [13]

This question is aimed at exploring what type of digital evidence will remain in Firefox's SQLite database after performing some interactions with the storage, how the extracted data can be interpreted for forensic timelines, and whether this approach will be sufficient for digital investigations.

Research Gap based on previous literature:

1. Cloud Storage Activity Detail: Previous research primarily works on identifying URLs and visit times; only a few will explore the detailed actions (folder creation, upload, and download). This research will explore and acknowledge this limitation. [12]
2. Specific Platform Forensics (Linux): Most existing research is focused on Windows-based browsers, and practical forensic cases are very rare in the Linux environment, especially using the Firefox browser.

3. Lack of Integrated SQL-Based Methodology: Amongst the previous research, only a few have provided the step-by-step SQL-based extraction for browser databases, but this research will show how to query places.sqlite and convert the result for forensic analysis.

4. Involvement of CLI tools in browser forensics: Most past research focused on GUI forensic tools, but here we will work on command-line analysis and scripting, which is replicable and powerful in this domain.

3.0 Methodology

The research methodology that is used in this paper is focused on digital forensic investigation and collection of web browser's evidence. Below are the tools used and system specifications:

3.1 Table 1: Tools and system setup used

Component	Details
System's Operating System	Linux Mint 21.2 Cinnamon
System's Hardware	Lenovo V15-IGL, Intel Celeron N4020, 4GB RAM
Forensic Tools	SQLite3, Autopsy
Web Browser	Mozilla Firefox

3.2 Procedural Forensic Workflow:

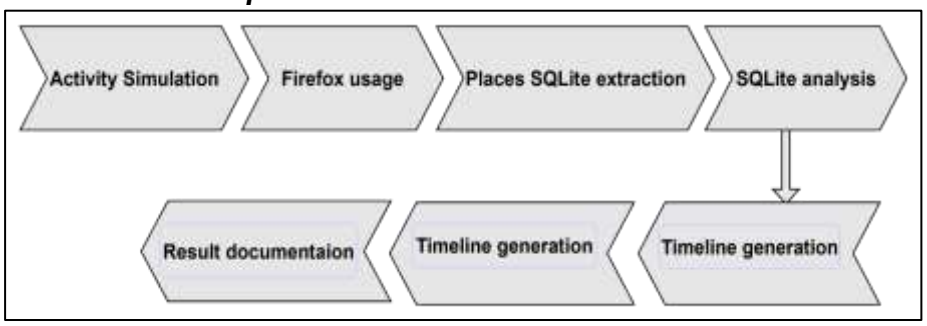

Fig 1: Forensic workflow

Fig:1 The image describe the procedural workflow of the research for visual representation of the process which includes: Activity simulation, Firefox usage, Places SQLite extraction, SQLite analysis, Timeline generation, and Result documentation.

The forensic procedural workflow: Linux Mint OS with the Firefox browser was used as a test environment, artifact collection was used to locate and copy 'places.sqlite,' timeline generation was used to create a documented report in ***.tsv*** format, and Autopsy was used to load the directory and extract the filtered result [14].

3.3 User Activity Simulation

A user logged in to his Google Drive account via the Firefox browser and performed certain actions, like creating a folder, uploading a file, and deleting files, to generate the browser artifacts.

3.4 Artifact Collection

The Firefox browser has stored the useful information needed in the.mozilla/firefox/<profile> directory. [6]

The key files include

Article I.cookies.sqlite: holds session cookies

Article II. places.sqlite: contains visited URL

Article III. cache2/entries: stores raw cache files

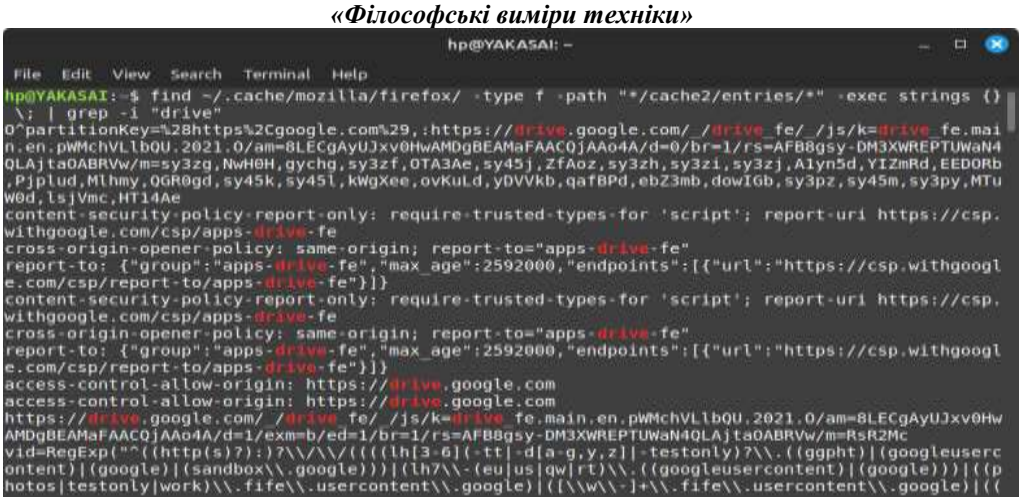

Fig 2: cache2/entries

Fig2: The image shows the cache data of the user's browser which can be used to extract the useful digital artifacts for analysis.

3.5 Sample SQL Query

SELECT datetime(moz_historyvisits.visit_) [3]

The command used:

cp ~/.mozilla/firefox/u4mtxaqy.default-release/places.sqlite ~/places_copy.sqlite

sqlite3 ~/places_copy.sqlite

.tables

SELECT url, title, visit_count FROM moz_places WHERE url LIKE '%drive%' [15] ;

And the following code was used to extract readable text in strings and grep:

strings ~/.cache/mozilla/firefox/*.default-release/cache2/entries/* | grep -i drive

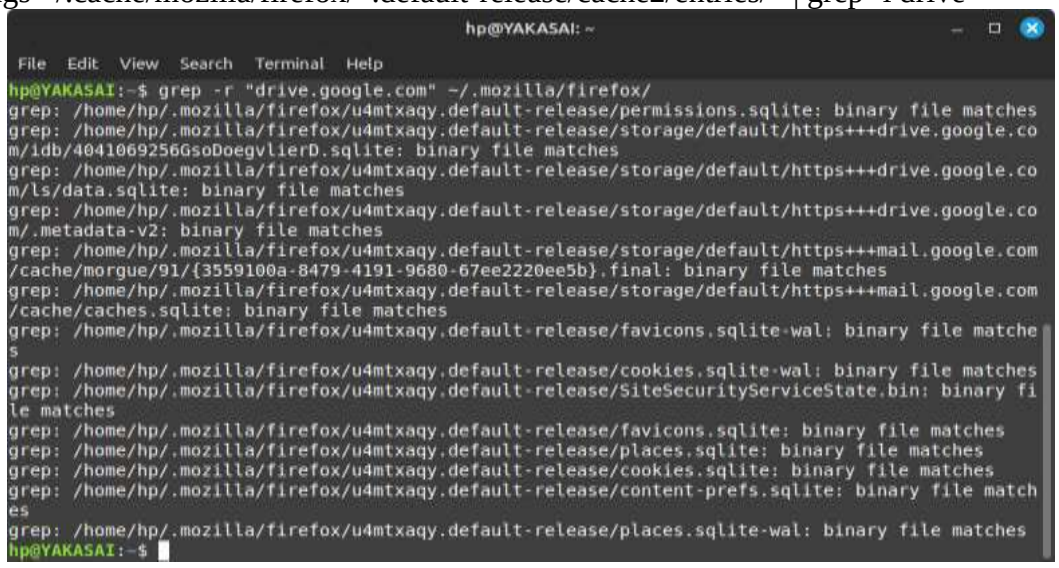

Fig 3: grep command for readable purpose

Fig3: The image displayed the grep command to extract the artifacts into human readable form, for analysis and investigation.

Autopsy Analysis: Autopsy (an open-source forensic tool) was used to import the browser directories and fetch the artifacts. The steps for the analysis: [16]

Article I.Open Autopsy > Create New Case

Article II. Add Data Source > Logical files

Article III. Select places.sqlite and cache2 directory

Article IV. View results in 'Web artifacts' and 'Interesting Files'

Fig 4: Autopsy software dashboard

Fig 4: The image shows the front page and dashboard of Autopsy software which includes: Case Gallery, Host Gallery, Host Manager, New Case, Main Menu, Description etc.

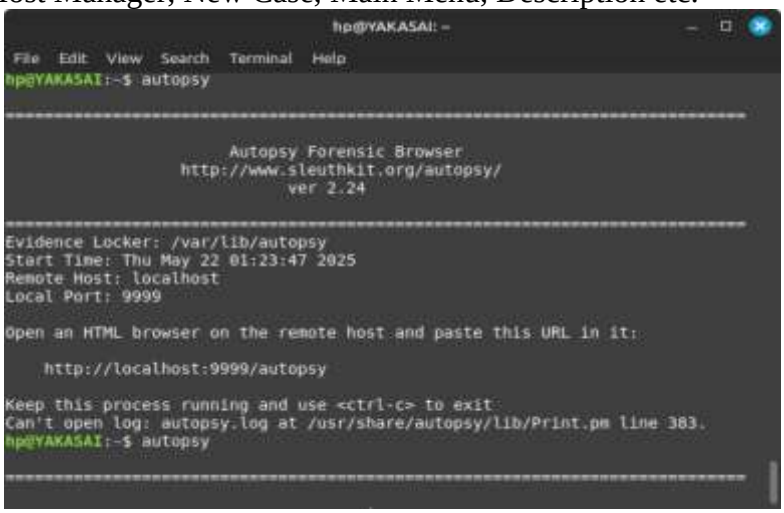

Fig 5: Autopsy connection with terminal for analysis

Fig 5: The image shows the connection of Autopsy software with system's terminal, this helps in collaboration between the two windows (Terminal and Browser)

Identifying the Profile Path

The Firefox browser profile was located by using the command:

ls ~/ .mozilla/firefox/ [8]

The profile folder normally ends in .default-release. Inside this folder, places.sqlite stores history, bookmarks, and session information.

Copying the SQLite File

The following command was used to copy the file:

cp ~/ .mozilla/firefox/u4mtxaqy.default-release/places.sqlite

~/ ~/ ~/places_copy.sqlite [

SQLite Command Line Analysis: Using SQLite3 CLI

sqlite3 ~/ ~/places_copy.sqlite

sqlite> .tables

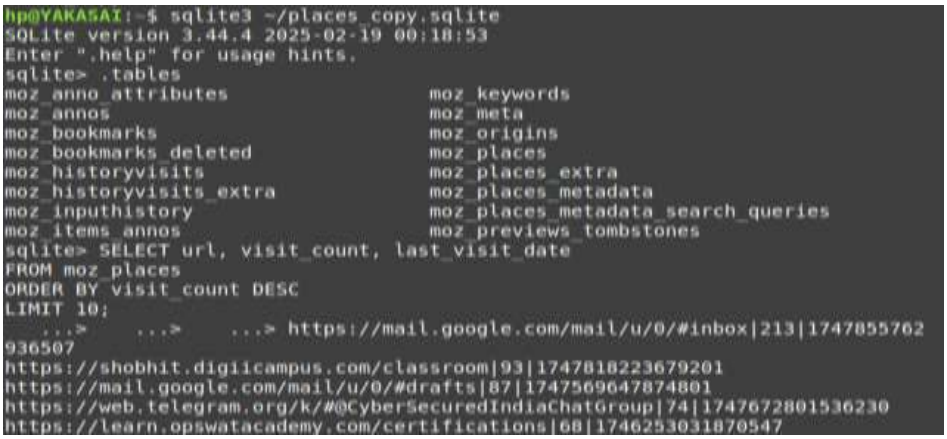

Fig 6: sqlite3 copying visited places

Fig 6: The image shows the command for copying the visited places of the user, using the browser artifacts.

Table 2: Forensic Tools Used

Tool	Purpose
SQLite3	Query and analysis of places.sqlite
Bash Commands	Copying of data and environment setup
Autopsy	GUI-based forensic timeline analysis

SQL Queries Used

The following query commands will extract all the Google Drive-related visits with timestamps:

```
SELECT datetime(moz_historyvisits.visit_date/1000000,'unixepoch') AS visit_time,
moz_places.url
FROM moz_places
JOIN moz_historyvisits ON moz_places.id = moz_historyvisits.place_id
WHERE url LIKE '%drive.google.com%'
ORDER BY visit_time DESC [3] ;
```

Fig 7: Extracting performed actions on Google Drive

Fig 7: The image shows the visited places and actions performed on the browser for analysis

Exporting the result in TSV format

sqlite3 -header -csv ~/places_copy.sqlite "<query>" > firefox_timeline.tsv

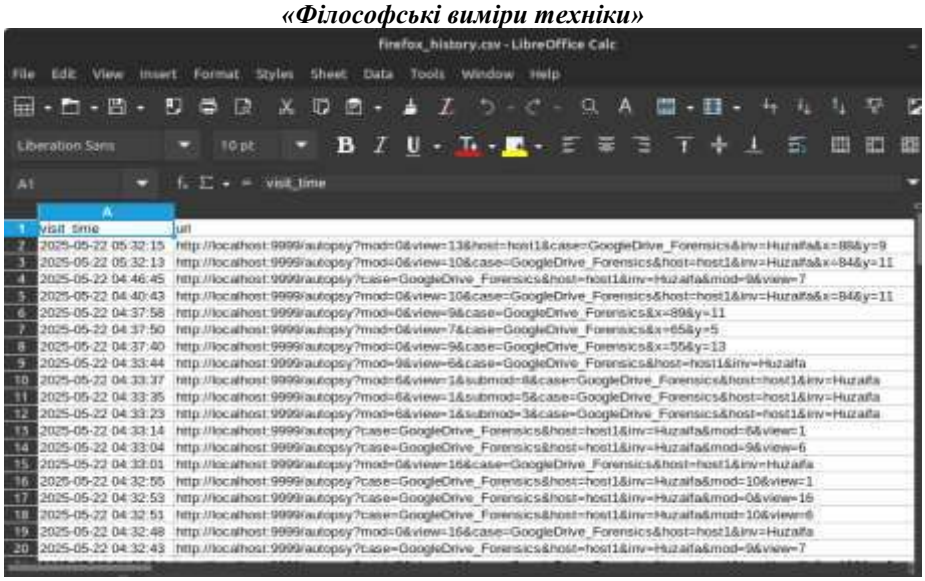

Fig 8: File in .tsv format

Fig 8: The image shows the saving format of the extracted artifacts into .tsv for arrangement of the artifacts and showing the visiting date and time of the user.

Organizing Artifacts

The artifacts were moved to a single folder for future reference and documentation:

mv firefox_timeline.tsv ~/firefox_artifacts/

4.0 Results and Analysis

The SQLite query successfully retrieved the historical records of the visits to Google Drive from the Firefox browser. Each visit entry included a URL and a timestamp, which form a reliable timeline. For example, entries with URLs like ‘https://drive.google.com/drive/my-drive’ were discovered. The file also was converted into human-readable timestamps. This data supports the profiling and evidence of cloud access at specific times. [18]

Table 3: Comparison of my research with previous research:

Prior Work	Description
Bagley et al. (2012): Recovery of SQLite artifacts from unallocated space in Firefox.	Demonstrates file-carving techniques to retrieve browser history databases even after deletion closely aligned with your Option 2 research.
Gupta & Mehtre (2013/14): Firefox in anti-forensic modes (sandbox/portable/virtual).	Explores trace persistence across hardened browsing modes and private sessions.
Sanghvi et al. (2024): Firefox forensic analysis across normal and private modes.	Compares data retrieval using FTK and Autopsy in RAM vs disk for cloud interactions.
International Journal of Digital Crime & Forensics (2025): Behavior comparison of Edge, Safari, Firefox using forensic tools.	Focuses on artifact retention across browsers and private mode challenges.
Reed et al. (2017): Epic Privacy Browser forensics case study.	Investigates evidence recovery from privacy-first browsers.

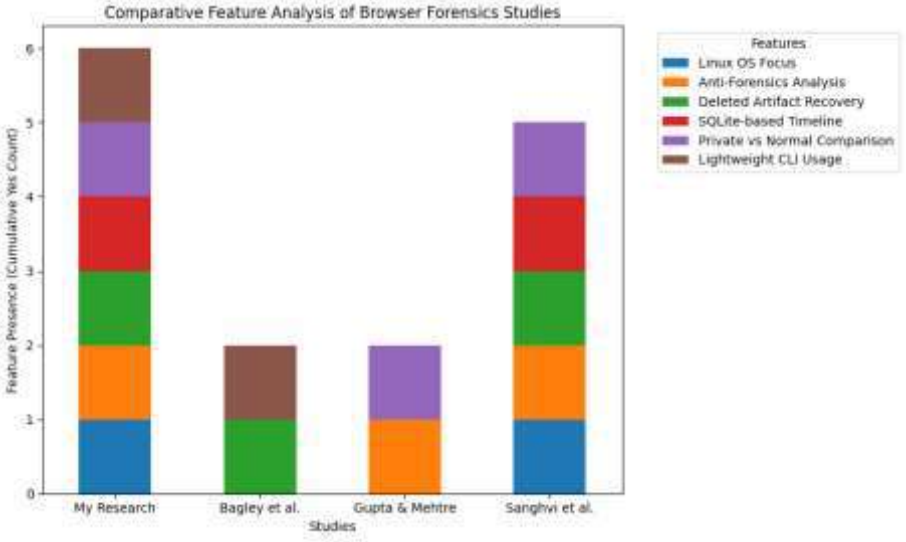

Fig 9: Research comparison chart

[19] [20] [21]

Fig 9: The image shows the comparison chart of this research and related past researches for visual representation.

Article I.Bagley et al. focus on low-level file recovery via carving, directly relevant to your plan using photorec/foremost.

Article II. Gupta & Mehtre evaluate anti-forensics modes, highlighting what user actions may still leave traces, which parallels your investigation of upload/delete artifacts.

Article III. Sanghvi et al. provide systematic comparisons of artifact persistence in Firefox normal vs. private mode using forensic tools, laying groundwork for your signal-vs-noise analysis.

Article IV. The ACM study (2025) provides modern context on multiple browsers and forensic tool performance useful for the "Related Work" section and justification of focusing on Firefox and SQLite CLI methods.

Article V. Reed et al. showcase privacy-oriented browser forensics, emphasizing how some artifacts may survive even in privacy tools.

5.0 Discussion

The use of SQLite and Autopsy in the browser's database to provide the ability to reconstruct a user's activity by investigation personnel, government surveillance and students that acquire knowledge on retrieving user's activity on Google Drive through artifacts has significant forensic implications, especially the approach used which shows the procedural workflow and steps to follow in order to acquire and achieve the goal which is retrieving user's activity on Google Drive using Firefox browser artifacts especially when the method was manually demonstrated, which provides transparency and flexibility, and by using a tool like Autopsy can help for further analysis, even though lightweight systems have compatibility issues [19] [2]. However, the method is limited by private browsing modes, encryption, and data overwrite which needs some advanced systems and tools for overcoming this problem and for deep analysis of the artifacts by experts and investigators.

6.0 Limitations

Session-Level Volatility: Some of the Google Drive activities occurred within transient JavaScript events or secured mediums that do not leave behind URL-based evidence. Autopsy Constraints on Linux:Autopsy's parsing modules provide minimal support to extract cloud-related browser activity when compared with full disk images or memory captures [24] [25].

During the investigation, forensics must be aware of those certain limitations and include additional techniques and methods for getting a better result on user activity [26].

7.0 Conclusion

This research reveals the feasibility of retrieving user's footprint and activities performed on Google Drive by using Firefox browser and the advantages of browser-based forensic investigation techniques on cloud storage usage by forensic investigation personnel or students for understanding the approach and techniques of retrieving browser artifacts by extracting browser's cache and converting the extracted file into human readable format for easy understanding analysis [18]. The browser's SQLite databases is preserving valuable evidences and browser's remnants, which includes the activities performed by a suspect which can be used for investigators to reconstruct users' timelines with appropriate methodologies. This technique will provide a foundational structure and highlight into browser-based cloud interactions for broader forensic investigations.

References

[1] T. Gros, R. Dirauf, and F. Freiling, "Systematic Analysis of Browser History Evidence," in *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, New York, NY, USA: IEEE, May 2020, pp. 1–12. doi: 10.1109/SADFE51007.2020.00010.

[2] E. Qazi, T. Zia, A. Alotibi, and S. Altaleedi, "Examining the Behavior of Web Browsers Using Popular Forensic Tools," *Int. J. Digit. Crime Forensics*, vol. 16, July 2024, doi: 10.4018/IJDCF.349218.

[3] "FQLite - SQLite Forensic Toolkit."

[4] F. Jamal and T. Siddiqui, "Comparative Analysis of Load Balancing Techniques in Cloud Computing, Based on LB Metrices," in *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India: IEEE, Oct. 2021, pp. 1–5. doi: 10.1109/ISCON52037.2021.9702508.

[5] A. W. Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou, and K.-I. Kim, "Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges," *Sensors*, vol. 24, no. 2, p. 433, Jan. 2024, doi: 10.3390/s24020433.

[6] A. A. Ahmed, K. Farhan, M. I. H. Ninggal, and G. Alselwi, "Retrieving and Identifying Remnants of Artefacts on Local Devices Using Sync.com Cloud," *Sensors*, vol. 25, no. 1, p. 106, Dec. 2024, doi: 10.3390/s25010106.

[7] E. Ramadhani and S. I. Isnaindar, "Digital Forensics in Google Drive: Techniques for Extracting and Analyzing Digital Artifacts," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 4, pp. 1203–1211, Aug. 2024, doi: 10.18280/ijsse.140417.

[8] M. M. Alshabibi, A. K. Bu Dookhi, and M. M. Hafizur Rahman, "Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review," *Computers*, vol. 13, no. 8, p. 213, Aug. 2024, doi: 10.3390/computers13080213.

[9] R. Shah, P. Shukla, D. Rathod, S. Hitesh, and Y. Zala, "Web Browser Forensics: Mozilla Firefox," *Int. J. Electron. Secur. Digit. Forensics*, vol. 1, p. 1, Jan. 2024, doi: 10.1504/IJESDF.2024.10055704.

[10] F. Jamal and M. Bansal, "Web Log Analyzer for Semantic Web Mining," vol. 6, 2015.

[11] C. A. Chhajed, "Comparison of Persistence of Deleted Files on Different File Systems and Disk Types," thesis, Purdue University Graduate School, 2024. doi: 10.25394/PGS.25639515.v2.

[12] R. Bagley, R. I. Ferguson, and P. Leimich, "FIREFOX BROWSER FORENSIC ANALYSIS VIA RECOVERY OF SQLITE ARTIFACTS FROM UNALLOCATED SPACE."

[13] M. F. Abdillah and Y. Prayudi, "Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux," *Int. J. Adv. Comput. Sci. Appl. IJACSA*, vol. 13, no. 9, Art. no. 9, Dec. 2022, doi: 10.14569/IJACSA.2022.0130975.

[14] S. Veerappampalayam Easwaramoorthy, S. Thamburasa, G. Samy, B. Bhushan S, and A. Karrothu, *Digital Forensic Evidence Collection of Cloud Storage Data for Investigation*. 2016. doi: 10.1109/ICRTIT.2016.7569516.

[15] A. Adesina, A. Adebiyi, and C. Ayo, "Detection and extraction of digital footprints from the iDrive cloud storage using web browser forensics analysis," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 26, p. 550, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp550-559.

[16] F. Focus, "Retrieving Digital Evidence: Methods, Techniques and Issues," Forensic Focus. Accessed: Mar. 13, 2025. [Online]. Available: https://www.forensicfocus.com/articles/retrieving-digital-evidence-methods-techniques-and-issues/

[17] R. Bagley, I. Ferguson, and P. Leimich, *Firefox Browser Forensic Analysis via Recovery of SQLite Artefacts from Unallocated Space*. 2012.

[18] "Autopsy - Digital Forensics."

[19] "Firefox Browser History for Forensic Investigations by Dean _ Medium."

[20] Prince Sultan University, A. Mahlous, H. Mahlous, and King's College London University, "Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, pp. 294–306, Dec. 2020, doi: 10.22266/ijies2020.1231.26.

[21] R. R. Chand, N. A. Sharma, and M. A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques," *SN Comput. Sci.*, vol. 6, no. 4, p. 355, Apr. 2025, doi: 10.1007/s42979-025-03921-6.

[22] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study," *Comput. Secur.*, vol. 115, p. 102626, Apr. 2022, doi: 10.1016/j.cose.2022.102626.

[23] R. R. Chand, N. A. Sharma, and M. A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques," *SN Comput. Sci.*, vol. 6, no. 4, p. 355, Apr. 2025, doi: 10.1007/s42979-025-03921-6.

[24] S. G. Punja and I. Whiffin, "Missing SQLite Records Analysis."

[25] "Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis" *Int. J. Res. Innov. Appl. Sci.*

[26] "Autopsy_Web Artifacts."

UDC: 004.056.53

Bello Bello Musa; Dr. Fakhrun Jamal; Huzaifa Sadi Yakasai
Scientific supervisor: Dr. Fakhrun Jamal, Assistant professor at cse department mmu mullana Haryana
Shobhit University, India

THE ROLE OF CYBER FORENSICS IN ENHANCING POLICE INVESTIGATION

Abstract*. This paper explores the vital importance of cyber forensics and how it plays a role in contemporary law enforcement investigations, weighing how it can be used to solve traditional daily crimes like terrorism, financial fraud, and murder. To prove how this digital evidence from social media footprints to blockchain transactions improves investigative accuracy and court results, the study looks at procedure, tools, and case studies. Important issues are inspected, such as jurisdictional difficulties, technology deficiencies in law enforcement, and new dangers like cryptojacking and deep fakes. The impact of the metaverse and artificial intelligence (AI) on forensic processes is also covered, which demands improved training and legislative changes. By facing these problems, the study hopes to advance the use of cyber forensics in law enforcement and guarantee justice in a society that is becoming more and more digital.*

Keywords: *cyber forensics, digital evidence, AI in policing, deep fakes, cryptojacking, and Metaverse investigations.*

Белло Белло Муса; д-р Фахрун Джамал; Хузаіфа Саді Якасаї
Науковий керівник: Д-р Фахрун Джамал, асистент-професор, Університет Махаріші Маркандешвара (MMU) у Муллані, штат Хар'яна, Індія