International Journal of Scientific Research in Multidisciplinary Studies
Vol.**10**, Issue.**10**, pp.**68-82**, October **2024**
E-ISSN: 2454-9312 P-ISSN: 2454-6143
Available online at: www.isroset.org

Research Article

Performance Evaluation of four Different Forensic Tools for Web Browser Analysis

Grace Bunmi Akintola[1*]

[1]Dept. of Cyber Security, Nigerian Defence Academy, Kaduna, Nigeria

**Corresponding Author:* gbogundele@nda.edu.ng

Received: 18/Aug/2024; **Accepted**: 20/Sept/2024; **Published**: 31/Oct/2024

Abstract— Advancements in digital technology have significantly increased the speed and convenience of internet use, enabling people to perform various tasks and activities through different web browsers. However, cybercriminals have exploited these advancements to carry out cybercrimes using multiple devices, including computers and mobile devices. The rise in cybercrime necessitates the adoption of digital forensics technologies and tools by law enforcement agencies to identify, acquire, process, analyze, and report electronically stored data from seized devices, tracking the suspect's online activities. This data can serve as admissible evidence in court if a forensic investigator conducts a thorough investigation. This paper evaluates and compares the performance of four forensic tools on a Windows 10 system using live data acquisition. The selected tools include Browser History Examiner (BHE), Browser History View (BHV), RS Browser, and OS Forensic, which were used to analyze five commonly used web browsers: Google Chrome, Microsoft Edge, Opera Mini, Internet Explorer, and Mozilla Firefox. The evaluation focuses on feature-based accuracy to determine which tools provide more valuable and substantial evidence during criminal investigations. Among the thirty-nine features identified across all tools, the OS Forensic tool demonstrated the highest accuracy, retrieving comprehensive browser data with an accuracy of 89.74% across four browsers (Google Chrome, Microsoft Edge, Internet Explorer, and Firefox). The RS Browser tool showed an accuracy of 71.79% across all five browsers, while BHE demonstrated an accuracy of 61.54% across Google Chrome, Microsoft Edge, Internet Explorer, and Firefox. BHV exhibited 33.33% accuracy across the four browsers.

Keywords— digital forensic, forensic tools, web browsers, Cybercrime, live acquisition data, digital forensic technology, web browser analysis

1. Introduction

With the advent of the internet in this digitalized era, the adoption of various web browsers has massively increased across all locations and regions. A web browser is simply described as a computer program or application used to navigate the internet. A browser is a software application that allows users to request and access web pages, images, videos, and multimedia content hosted on web servers across the internet [1]. It is the main way to access information available on the internet. Today, millions of people rely on web browsers to search for information, check emails, conduct online transactions, download educational materials, engage in social networking, perform online banking, and more [1].

There are various examples of web browsers used by people to access the internet for several online activities, including Google Chrome, Mozilla Firefox, Opera Mini, Microsoft Edge, Internet Explorer, Safari, and more [2]. Internet users utilize web browsers for several activities depending on their motivations, which can be positive or negative. Since anyone from anywhere in the world can operate and navigate the internet through the web browser to request and receive information about people, places, organizations, and more, it can also be leveraged by cybercriminals to gather information about their online victims which can be used to commit further digital crimes.

In view of this, several law enforcement agencies are being established by different countries to investigate and detect criminal activities as well as enforce the founded laws on criminals. Examples include, but are not limited to, the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA)., EFCC (Economic Financial Crime Commission), Police, and NDLEA (National Drug Law Enforcement Agency) [3]. In the process of the investigation of crimes committed by several criminals online, the adoption of digital forensic technology became extremely needed to enhance and produce accurate investigations [4].

Digital Forensics functions as a science, using thorough procedures to investigate digital artifacts and reveal evidence while adhering to established scientific principles. Digital

Forensics (DF) is also a branch of forensic science focused on revealing and analyzing digital data. It primarily involves the discovery, validation, and interpretation of digital evidence related to digital crimes [5]. The technique for testing in Digital Forensics is to reflect the systematic and empirical nature of the scientific method, ensuring investigations are structured, reproducible, and dependable. Applying the scientific method helps Digital Forensics practitioners formulate hypotheses, conduct controlled experiments, and perform unbiased data analysis. This approach upholds scientific standards, enhances the reliability and integrity of findings, and supports the accuracy and validity of investigative outcomes [6]. Generally, the forensic process starts from the collection stage to the identification process, to the preservation stage, to the analysis stage, to the documentation stage, and finally, to the presentation stage [7]. Digital evidence intended to be identified, preserved, analyzed, and documented by the digital forensic analyst can be stored on various devices, such as thumb drives, cell phones, hard drives, CDs, DVDs, digital cameras, pen drives, and more.

To analyze the evidence obtained by the forensic examiner at the crime scene for proper investigation, several available forensic tools can be adopted depending on the digital forensic type including mobile forensics, network forensics, database forensics, and much more. Therefore, this paper focuses on evaluating and comparing the performances of four different forensic tools used for web browser analysis.

2. Related Work

2.1 Overview of web browsers

Web browsers are among the most frequently used applications by computer users. Users perform various tasks through web browsers, such as accessing the internet, downloading files, using social media platforms, and managing email accounts [8]. However, while browsers are vital for a productive working environment, they also present an ideal target for cyberattacks. As more services become available online, the need for fast and secure access to resources has become increasingly important. The internet's growth has driven many people to explore and utilize the World Wide Web (www). Since the web browser serves as the gateway to the www, this demand has led to the development of various web browsers in today's market. [9]**.** Furthermore, research shows that users' reliance on the internet grows daily, correlating with the increasing number of online services. As internet usage continues to rise, more users are eager to explore and make full use of its offerings. The primary way for users to access the World Wide Web is through a web browser, leading to the development of numerous browsers to meet this demand [10]. Common examples of web browsers widely used on Mobile devices include but are not limited to Google Chrome, Safari, Samsung Internet, Opera, UC browser, and Firefox. In contrast, examples of desktop browsers are not limited to Google Chrome, edge, safari, opera, 360 Safe, and Firefox [10]. The increasing usage of web browsers either on mobile devices or desktops has given leverage for cybercriminals to perpetrate all forms of crimes online either through a mobile device or desktop, hence leading to the need for forensic experts to analyze any seized suspect's devices to obtain valuable pieces of evidence through the use of various compatible forensic tools.

2.2 **Overview of digital forensics (types, process, advantages, and challenges)**

Digital forensics, a critical field in the scientific examination and analysis of digital device data, has gained increasing relevance as technology becomes more pervasive. It has firmly established itself as a cornerstone in the technological era, playing a vital role in cybersecurity and legal proceedings. Its significance in today's interconnected digital world cannot be overstated. [11]

Traditionally, digital forensics is defined as the systematic, scientifically rigorous process of examining, preserving, extracting, and documenting digital evidence, primarily for use in legal or administrative proceedings. This broad field covers various devices and platforms, including traditional computer systems, mobile devices, network traffic, and the rapidly growing Internet of Things (IoT). As technology continues to penetrate nearly every aspect of personal and professional life, a structured, methodological approach to examining digital evidence has become essential. The rise in cybercrime and the challenges of tracing digital footprints highlighted the urgent need for specialized skills and techniques to retrieve and preserve digital evidence in its original state, ensuring its admissibility in court. [11]

Several researchers generally explained the various categories of which digital forensics are expanded but not limited to network forensics, mobile forensics, disk and storage devices forensics, cloud forensics, e-mail forensics, IoT forensics, Darkweb forensics, Bid Data digital forensics, digital video/Audio forensics, and computer forensics, web forensic [12].

Despite the numerous advantages of the application of digital forensics to discovering all forms of valuable information from the seized devices through adhering to the different designed forensic process based on an individual's view and research, thus, helping in a criminal investigation as admissible evidence in the court of law, several challenges have been discovered over the years, which were categorized into five (5) groups: technical, legal, operational, investigative, and resource challenges [12].. The Legal challenges posed by the adoption of digital forensics include the rapid pace of technological advancement that has outpaced laws, which often experienced difficulty in keeping up with emerging digital devices, cloud storage solutions, and encryption methods. This lag produces obscurity surrounding the legality of certain investigative techniques and Privacy and jurisdictional issues [13]. The operational challenge in the application of digital forensics includes the Increased use of encryption which makes it challenging to access and analyze data, requiring advanced decryption techniques that may not always be feasible. The resource challenges include the high cost of forensic tools and equipment needed for effective investigation by forensic analysts. Lastly, one of the technical challenge aspects involves Data Volume which means that as the digital realm has expanded, so has the immense amount of data generated, stored, and transmitted by devices. The proliferation of digital devices, along with their ever-increasing storage capacities, means that forensic practitioners frequently face the task of navigating vast amounts of data. This growth is exponential rather than linear, making it one of the most important technical challenges in digital forensics [14].

2.3 Related works on various techniques for browser forensic analysis and tools

The analysis of Brave's private browsing mode was conducted, focusing on its privacy features and forensic data acquisition. Various types and locations of evidence available were explored through live and post-mortem state analysis. Our unique approach involved conducting experiments to reveal how the browser operates and identifying tools that could be used to extract residual artifacts. The results showed that, while Brave leaves no traces of browsing activity on the hard disk, visited URLs, images, keyword searches, and even cached videos were recoverable from RAM. This indicates that Brave's private browsing mode is not entirely private [15]

A comprehensive methodology for identifying and collecting artifacts related to browsing activities on Firefox, Chrome, and Edge in Windows 11. The approach involves analyzing each stage of browser usage, including installation, execution, uninstallation, and abnormal behaviors like crashes and restarts. Simulated cybercriminal activities are employed to gather artifacts at each stage, which are then examined using Windows 11 components such as the registry, memory, storage, and log files. The experimental results highlight vulnerabilities, including crashes, that may result in the loss of sensitive information. This methodology offers a strong foundation for improving browser forensic analysis and enhancing cybercrime investigations [16].

While Mozilla Firefox was running in both normal and private modes, a thorough investigation was performed to evaluate the status of the evidence. The experiment involved performing activities on one virtual machine in regular mode and another in a private Firefox window. Following this, we conducted a forensic acquisition of the RAM and hard drive to assess the types of evidence recovered from both VMs. We used the tools FTK and Autopsy to analyze the collected data. Our findings revealed significant evidence of various activities related to Google, YouTube, Twitter, Amazon, Facebook, Outlook, Yahoo, and Gmail, obtained through hard disk and RAM forensics in both modes. The results also indicated that FTK extracts more data from the image file than Autopsy [17].

Another study was conducted which involved examining the use of private mode and browsing artifacts across four popular web browsers: Google Chrome, Edge, Mozilla Firefox, and Brave, with a focus on analyzing both hard disk and random access memory. Forensic analysis of the target device confirmed that using private mode aligned with each browser vendor's claims, indicating that browsing activity, search history, cookies, and temporary files are not saved to the device's hard disk. However, in volatile memory analysis, a significant number of artifacts were recovered from the test cases. This suggests that a malicious hacker employing a similar procedure could potentially access the remnants of confidential information on the device without the user's consent [18].

This paper introduces a novel methodology for reconstructing searched keywords from the physical memory dump collected from the suspect's Windows 10 computers. It also outlines a method for retrieving keywords from browser files stored on the media. The keywords obtained through this process assist investigators in identifying critical information during the in-depth analysis of storage media in offline forensic investigations [19].

Another research was conducted to investigate the validity of claims made by web browser companies regarding the level of protection offered by private browsing and whether it truly leaves no browsing data behind. We analyzed the most popular desktop browsers—Google Chrome, Mozilla Firefox, and Edge—on Windows, both in regular and private modes. The results indicate that the level of privacy supplied differs among many companies, as evidence could be recovered from some browsers but not from others [20].

3. Research Methodology

3.1 Justification of the applied research method

For this research which involves the use of four different browser forensic tools for analyzing web browsers, a quantitative research methodology was chosen due to its easy interpretation of the obtained data (results) based on the selected features for all the chosen web browsers. Another advantage of using a quantitative method for the research is its high level of accuracy which helps in making a solid decision and conclusion of the research work [21]

3.2 Justification of the selected web browsers

According to the recent study conducted by Oberlo, on internet browser market share by device, it was revealed on the most widely used web browsers by users around the world. The usage of Google Chrome browser on the desktop shows 64.55%, followed by Microsoft Edge's 13.80%. The Safari browser shows usage of 9.38%, the Mozilla Firefox browser reveals 6.66%, the Opera mini shows 2.41% while the 360 safe browser depicts 1.12%. For this paper, only five browsers were selected and analyzed: Google Chrome, Mozilla Firefox, Opera Mini, and Internet Explorer [22].

Google Chrome was chosen due to its easy user interface, high-speed browsing, security, customizability, and device synchronization. Microsoft Edge was also selected due to its additional built-in features which enhance your browsing experience with world-class performance and speed, optimized specifically for Windows. It includes advanced security features to help keep you and your loved ones protected online. Additionally, Edge incorporates AI-powered tools that improve your browsing experience, such as a side-by-side view for easier and faster shopping, detailed answers, information summarization, and discovering new inspiration—all without the need to switch tabs or leave your browser. Although Safari browser is shown to be more widely used than Mozilla Firefox according to Figure 1 but was not selected due to its lack of built-in protection against malware and phishing features (automatically blocking dangerous downloads and warning users if they attempt to visit a malicious site) in which Mozilla Firefox has, thus, offering a significant advantage over Safari. Mozilla Firefox was also selected due to its speed and performance, offering quick page-loading times and efficient memory usage. Additionally, Firefox places a strong emphasis on user privacy and security, featuring enhanced tracking protection and automatic blocking of known malicious websites.

Opera mini browser was selected as well due to its built-in ad blocker which prevents intrusive advertisements, leading to a smoother browsing experience and safeguarding your privacy from tracking cookies often employed by advertisers. Additionally, Opera Mini's advanced security features offer protection against malicious websites and phishing attempts. Finally, the Internet Explorer browser was selected due to its user-friendly interface, which is easy to navigate, making it accessible even for novice users. Its clean and intuitive design enables users to quickly locate necessary features and customize their browsing experience to suit their preferences. It was chosen over the 360 safe browser as shown in Figure 1 as a result of its compatibility with paid antivirus clients, forced advertising features, and challenges in configuration and removal, particularly for non-Chinese users (users) with Internet Explorer.

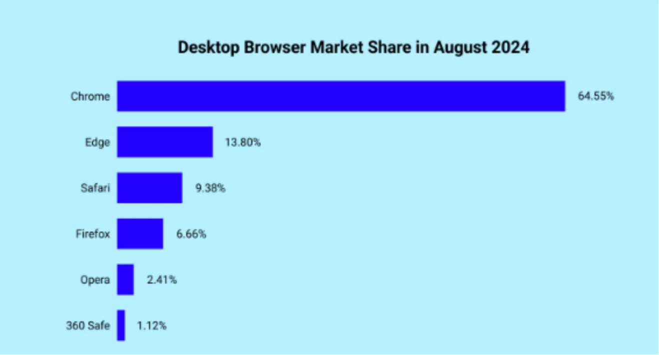


Figure 1: The most frequently used desktop browser in 2024 [22]

3.3 Forensic procedure for the analysis

In performing the forensic investigation of the selected web browsers using four (4) different web browser forensic tools namely: Browser History Examiner tool, Browser History View, RS Browser Forensics tool, and OS (Operating System) Forensic tool, the standard Five-step forensic process for analysis was followed and these include: data identification, data acquisition, analysis, documentation and reporting [23]

i. **Data identification:** This stage involves identifying the particular media or device where the needed data for the analysis are stored. In this paper, the identified data was stored on the "**C:\Users**" file path in the local disk of the Windows 10 operating system.

ii. **Data (Live) Acquisition:** the next stage is to acquire the already identified data which can be done generally using two methods: static and live acquisition in this research a live acquisition method was adopted because live imaging can be faster and more convenient than dead imaging, especially when remote access to the system or device is available. One key advantage of live imaging is its ability to capture volatile data in real-time, allowing the examination of running processes. This approach provides forensic analysts with a comprehensive view of how the system was used immediately before the imaging process. In contrast, with a static approach, this critical volatile data is lost when the system is shut down, preventing access to potentially important electronically stored information (ESI). Live acquisition is proactive and preventative, rather than reactionary and retrospective. Another reason for adopting the live acquisition approach was due to the large memory size of the data which can result in fragmentation when being imaged by the Forensic imaging tool [24]**.**

iii. **Analysis:** This stage deals with the analysis of the acquired data using the selected web browser forensic tools. This involves analyzing based on selected features in the web browsers across all the forensic tools to evaluate their functionalities and performances which help in creating well-cleared and understandable documentation and reporting to the appropriate Law agencies as a digital forensic analyst.

iv. **Documentation:** this stage involves gathering and creating a well-cleared and understandable writing of the report. The investigative insights are properly documented in a manner that visualizes the entire investigative process and its conclusions.

v. **Reporting:** Finally, this stage involves presenting the findings to a court, committee, or group responsible for determining the result of a lawsuit or internal complaint. Digital forensics investigators may act as expert witnesses, outlining and delivering the evidence they have identified and revealing their findings.

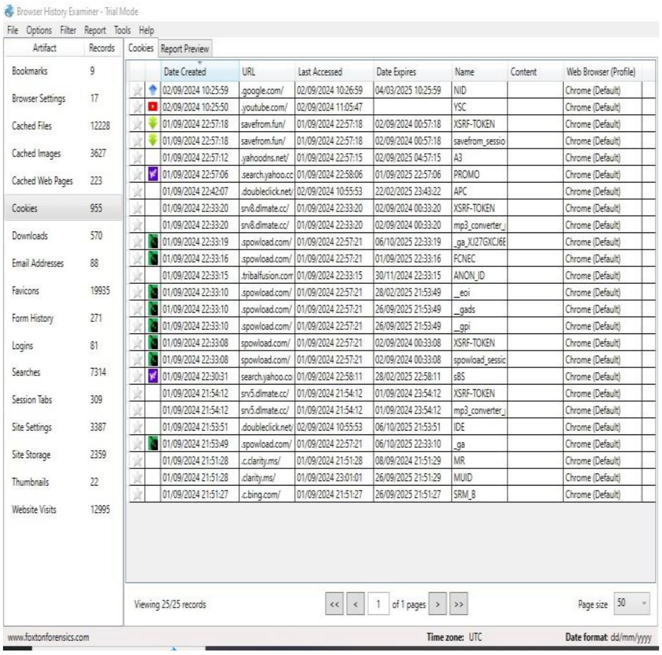
3.4 Justification of the selected web browser forensic tools

i. BHE (Browser Forensic Examiner) tool:

Browser History Examiner (BHE) is described as a forensic software tool designed for collecting, evaluating, and documenting internet history from major desktop web browsers. It is selected due to its valuable effect in a range of digital investigations, including civil and criminal digital forensics, security incidents, human resources investigations, and general employee activity reporting. It enables forensic investigators to easily acquire browser history from live Windows and macOS computers, as well as automatically extract browser history from Windows or macOS forensic image files. [25]

BHE trial version (v1.20.6) was used in this paper for live acquisition of data on the Windows 10 operating system as illustrated in Figure 2 in which the captured view of all the web browser data in Browser History Examiner after the following procedures have been followed:

Step1: Open the Browser History Examiner tool and select the “capture history”
Step 2: Click on the “next” button
Step 3: check on all the available “web browsers” and data to be captured
Step 4: Select the destination folder where the report will stored on the system
Step 5: click on the “capture” button and the extraction of data starts
Step 6: Click to view the whole captured data after the extracting process is finished.


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Cookies
Report Preview

Artifact	Records
Bookmarks	9
Browser Settings	17
Cached Files	12228
Cached Images	3627
Cached Web Pages	223
Cookies	955
Downloads	570
Email Addresses	88
Favicons	19935
Form History	271
Logins	81
Searches	7314
Session Tabs	309
Site Settings	3387
Site Storage	2359
Thumbnails	22
Website Visits	12995

Date Created	URL	Last Accessed	Date Expires	Name	Content	Web Browser (Profile)
02/09/2024 10:25:59	.google.com/	02/09/2024 10:26:59	04/03/2025 10:25:59	NID		Chrome (Default)
02/09/2024 10:25:50	.youtube.com/	02/09/2024 11:05:47		YSC		Chrome (Default)
01/09/2024 22:57:18	savefrom.fun/	01/09/2024 22:57:18	02/09/2024 00:57:18	XSRF-TOKEN		Chrome (Default)
01/09/2024 22:57:18	savefrom.fun/	01/09/2024 22:57:18	02/09/2024 00:57:18	savefrom_sessio		Chrome (Default)
01/09/2024 22:57:12	.yahoodns.net/	01/09/2024 22:57:15	02/09/2025 04:57:15	A3		Chrome (Default)
01/09/2024 22:57:06	.search.yahoo.cc	01/09/2024 22:58:06	01/09/2025 22:57:06	PROMO		Chrome (Default)
01/09/2024 22:42:07	.doubleclick.net/	02/09/2024 10:55:53	22/02/2025 23:43:22	APC		Chrome (Default)
01/09/2024 22:33:20	srv8.dlmate.cc/	01/09/2024 22:33:20	02/09/2024 00:33:20	XSRF-TOKEN		Chrome (Default)
01/09/2024 22:33:20	srv8.dlmate.cc/	01/09/2024 22:33:20	02/09/2024 00:33:20	mp3_converter_		Chrome (Default)
01/09/2024 22:33:19	.spowload.com/	01/09/2024 22:57:21	06/10/2025 22:33:19	_ga_XJ27GXCJ6E		Chrome (Default)
01/09/2024 22:33:16	.spowload.com/	01/09/2024 22:57:21	01/09/2025 22:33:16	FCNEC		Chrome (Default)
01/09/2024 22:33:15	.tribalfusion.com	01/09/2024 22:33:15	30/11/2024 22:33:15	ANON_ID		Chrome (Default)
01/09/2024 22:33:10	.spowload.com/	01/09/2024 22:57:21	28/02/2025 21:53:49	__eoi		Chrome (Default)
01/09/2024 22:33:10	.spowload.com/	01/09/2024 22:57:21	26/09/2025 21:53:49	__gads		Chrome (Default)
01/09/2024 22:33:10	.spowload.com/	01/09/2024 22:57:21	26/09/2025 21:53:49	__gpi		Chrome (Default)
01/09/2024 22:33:08	spowload.com/	01/09/2024 22:57:21	02/09/2024 00:33:08	XSRF-TOKEN		Chrome (Default)
01/09/2024 22:33:08	spowload.com/	01/09/2024 22:57:21	02/09/2024 00:33:08	spowload_sessic		Chrome (Default)
01/09/2024 22:30:31	search.yahoo.co	01/09/2024 22:58:11	28/02/2025 22:58:11	sBS		Chrome (Default)
01/09/2024 21:54:12	srv5.dlmate.cc/	01/09/2024 21:54:12	01/09/2024 23:54:12	XSRF-TOKEN		Chrome (Default)
01/09/2024 21:54:12	srv5.dlmate.cc/	01/09/2024 21:54:12	01/09/2024 23:54:12	mp3_converter_		Chrome (Default)
01/09/2024 21:53:51	.doubleclick.net/	02/09/2024 10:55:53	06/10/2025 21:53:51	IDE		Chrome (Default)
01/09/2024 21:53:49	.spowload.com/	01/09/2024 22:57:21	06/10/2025 22:33:10	_ga		Chrome (Default)
01/09/2024 21:51:28	.c.clarity.ms/	01/09/2024 21:51:28	08/09/2024 21:51:29	MR		Chrome (Default)
01/09/2024 21:51:28	.clarity.ms/	01/09/2024 23:01:01	26/09/2025 21:51:29	MUID		Chrome (Default)
01/09/2024 21:51:27	.c.bing.com/	01/09/2024 21:51:27	26/09/2025 21:51:27	SRM_B		Chrome (Default)

Viewing 25/25 records

www.foxtonforensics.com Time zone: UTC Date format: dd/mm/yyyy

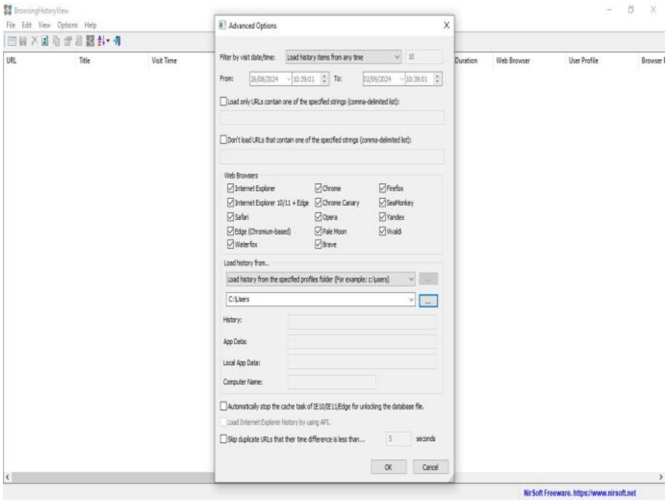
Figure 2: view of web history in the BHE forensic tool

ii. BHV (Browser History View) tool:

Browsing History View is one of the selected forensic tools that reads and consolidates browsing history data from various web browsers, including Google Chrome, Opera, and others, into a single table. The table displays key information such as visited URLs, page titles, visit times, visit counts, web browser used, and associated user profiles. This tool enables you to view browsing history from all user profiles on a running system, as well as obtain history from an external hard drive [26].

Figure 3 depicts the full process of using the BHV forensic tool for the live acquisition of web browser data of the suspect’s system. The step-by-step procedure for applying the Browser History View forensic tool includes:

1. Open the BHV tool and select the filtering date and time where you want the captured data to start and end
2. Select the preferred web browsers you want to analyze
3. Select the drop-down menu and load history from the specified profiles folder “**C:\Users”**
4. Click on the “Ok” button at the bottom of the window
5. Click on the “view” button to scroll through the captured data and then save it as “Report” in the compatible format.



Filter by visit date/time: Load history items from any time 10
From: 26/08/2024 10:39:01 To: 02/09/2024 10:39:01
☐ Load only URLs contain one of the specified strings (comma-delimited list):
☐ Don't load URLs that contain one of the specified strings (comma-delimited list):

Web Browsers
☑ Internet Explorer ☑ Chrome ☑ Firefox
☑ Internet Explorer 10/11 + Edge ☑ Chrome Canary ☑ SeaMonkey
☑ Safari ☑ Opera ☑ Yandex
☑ Edge (Chromium-based) ☑ Pale Moon ☑ Vivaldi
☑ Waterfox ☑ Brave

Load history from..
Load history from the specified profiles folder (For example: c:\users)
C:\Users
History:
App Data:
Local App Data:
Computer Name:
☐ Automatically stop the cache task of IE10/IE11/Edge for unlocking the database file.
☐ Load Internet Explorer history by using API.
☐ Skip duplicate URLs that their time difference is less than... 5 seconds

NirSoft Freeware. https://www.nirsoft.net

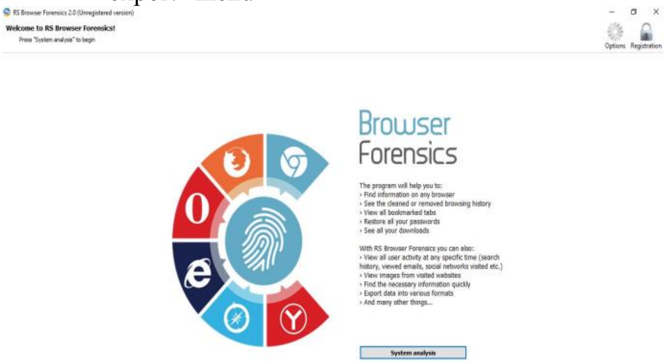
Figure 3: procedures for web history loading into the BHV forensic tool

iii. RS Browser tool

RS Browser Forensics was selected due to its features such as extracting, recovering, and analyzing data from popular web browsers. It can access deleted browsing history and investigate incognito sessions through a low-level hard drive scan. The tool recovers stored logins, passwords, and bookmarks and gathers additional information about the user's online activities. Even if the browsing cache has been cleared, RS Browser Forensics can retrieve user activity traces by thoroughly scanning the disk. Its advanced disk analysis engine detects both current and previously used web browsers, uncovering traces of private browsing sessions and deleted browsing history [27]. Figure 4 illustrates the user interface of the RS browser tool which can be used by either “registered” or “unregistered” users for web browser analysis. However, the “unregistered” version was used for this paper due to its high cost.

The step-by-step procedure for using the RS browser forensic tool is as follows:

a. Open the RS browser Forensic tool
b. Click on the “ system analysis” button
c. Select the “user” profile of the system to be analyzed
d. Select the particular web browser to be analyzed one after the other
e. After viewing the whole web history and activities, you can export the generated data by clicking on the “export” menu



Welcome to RS Browser Forensics!
Press "System analysis" to begin

The program will help you to:
› Find information on any browser
› See the cleaned or removed browsing history
› View all bookmarked tabs
› Restore all your passwords
› See all your downloads

With RS Browser Forensics you can also:
› View all user activity at any specific time (search history, viewed emails, social networks visited etc.)
› View images from visited websites
› Find the necessary information quickly
› Export data into various formats
› And many other things...

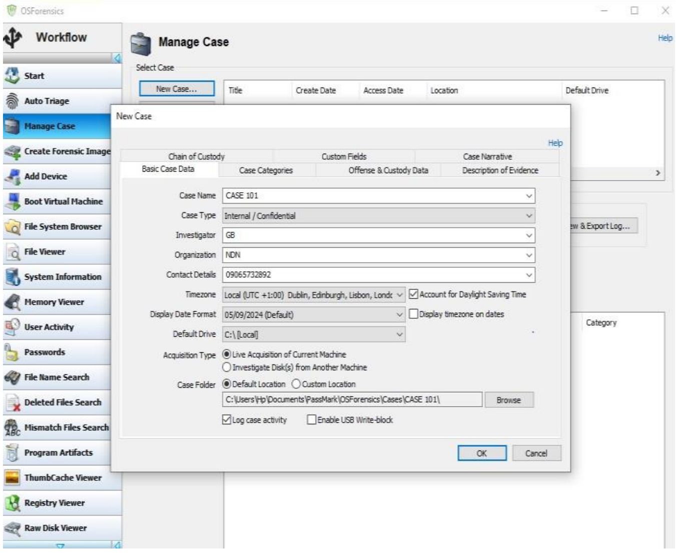
Figure 4: The use interface of the RS browser forensic tool

iv. OS forensic tool

OS Forensics provides a comprehensive analysis of various aspects of computers to support digital investigations. It is known for its fast search capabilities, efficiently handling vast amounts of data. The tool also includes password recovery features, which can be crucial in investigations. OS Forensics allows users to add a wide range of items to their cases, such as traditional files, file lists, third-party reports, evidence photos, chain of custody information, and the OSF case log. Additionally, it enables users to "tag" files during examination for further analysis, and these tagged files can be easily added to the case for review [28].

Figure 5 shows the interface of the OS forensic tool which describes the processes taken for the analysis of the web browsers to enable forensic investigators to obtain well-detailed and in-depth reports. The procedures for using OS forensic tools are as follows:

i. Open the OS forensic tool
ii. Click on the “new case” button to create a case for analysis to be done
iii. Select the time zone to be used for the investigation
iv. On the acquisition type, select “live acquisition on the current machine”
v. Browse the case folder and click “ok”.



Case Name: CASE 101
Case Type: Internal / Confidential
Investigator: GB
Organization: NDN
Contact Details: 09065732892
Timezone: Local (UTC +1:00) Dublin, Edinburgh, Lisbon, Londc ☑ Account for Daylight Saving Time
Display Date Format: 05/09/2024 (Default) □ Display timezone on dates
Default Drive: C:\ [Local]
Acquisition Type: ● Live Acquisition of Current Machine ○ Investigate Disk(s) from Another Machine
Case Folder: ● Default Location ○ Custom Location
C:\Users\Hp\Documents\PassMark\OSForensics\Cases\CASE 101\
☑ Log case activity □ Enable USB Write-block

Figure 5: The OS forensic tool interface and procedure

4. Results and Discussion

4.1 Criteria of features identified across all the web browser forensic tools

i. **Compatible browsers:** This feature indicates the number of web browsers that were compatible and viewed by each of the forensic tools adopted for the analysis. As discussed in **section 3** of the five selected web browsers.

ii. **Browser settings (profile):** A set of parameters is configured when a profile is created, which determines the information websites and services receive about the particular system to generate a fingerprint [29].

iii. **Export data formats**: This indicates the file format in which the generated report from each forensic tool can be exported for proper documentation by the forensic analyst.

iv. **Login details**: this feature indicates the user’s login data for accessing various websites and services on web browsers which was identified by the forensic tools.

v. **Password recovery:** this feature was used to assess the selected forensic tool’s capacity to view the list of stored passwords on web browsers used by the user of the analyzed system and the deleted passwords that can be used for further investigation.

vi. **Form History:** This shows Form history all forms of the data the user entered into web page forms for autocomplete purposes. This can be used as part of understanding the user’s activities for investigation [30]

vii. **Email messages extraction:** this deals with viewing, accessing, and reading all the email messages on the analyzed web browsers through the forensic tool which helps in gaining more substantial evidence

viii. **Support Keyword Search:** this deals with being able to search for some keywords by the forensic analyst while viewing through the captured data.

ix. **Timeline analysis:** this feature deals with analyzing a series of data points gathered over a specific time interval on the visited websites by the user. This extension enables users to track and analyze their website usage, providing detailed insights into how much time is spent on each site daily. It helps users gain a better understanding of their online habits.

x. **Extracting artifacts from a web browser:** this deals with extracting various data stored by the used web browsers, generally saved in a particular folder within the operating system, hence, serving as a digital clue of the suspect during the investigation.

xi. **Hash set filtering:** This filtering process relies on hash calculations. Typically, a hash is computed for each file in the image and compared against a pre-established list of hashes generated from known legitimate files.

xii. **Downloads:** this shows all the downloaded files stored which can be either in images, audio, video, or documents that can be viewed to further track the user’s activity.

xiii. **Site storage:** This feature is also referred to as DOM storage (Document Object Model storage), this is a standard JavaScript API provided by web browsers. It allows websites to store persistent data (data are consistently fetched by the user on the website) on users' devices, similar to cookies but with a larger capacity and without sending information in HTTP headers.

xiv. **Session tabs:** The Session tab represents a tab or window that the user has closed during the current browsing session. Tabs that were closed without closing their window, such as when a user clicks the "Close tab" button while other tabs remain open, are represented as Tab objects. The forensic analyst can use this to track the several session tabs the user opened and closed and the web pages he/she accessed as part of the user's activity.

xv. **Favicons:** Favicons, short for "favorite icons," are small images typically displayed on browser tabs, bookmark bars, browsing history, and search results next to the page URL. These files contain one or more icons associated with a specific website or webpage, helping users quickly identify a website among multiple open tabs or in their browser history. Favicons can also serve as a valuable source of information during forensic investigations, providing additional insight into the websites or locations visited.

xvi. **Website visits (counts):** This displays the number of times the user of the analyzed system visits a particular website. This can help the digital forensic investigator better understand the user's activity.

xvii. **URL (Uniform Resource Locator) length:** A URL (Uniform Resource Locator), also known as a web address, is a unique identifier used to locate a resource on the internet. It consists of several components, such as protocol and domain name, which guide web browsers on how and where to access the resource. URL length is important because it affects user experience and search engine optimization (SEO). Short, readable URLs improve user experience thus, facilitating visitors to understand the content and purpose of a webpage quickly. The URL length can also be of great help to forensic investigators as it can help for easy navigation to various visited websites.

xviii. **Site setting:** Site settings are stored in the Preferences file, which is a JSON file typically located in a specific directory on a Windows machine. Each setting includes a URL and a Last-Modified timestamp. During testing, URLs were found in these settings that no longer appeared in the standard web history, making this a useful source for uncovering additional evidence for the digital forensic investigator about the websites the user may have interacted with. However, testing also revealed identical Last Modified timestamps for multiple websites, suggesting that this timestamp may indicate when the browser updated the Preferences file, rather than the precise moment the setting was last changed.

xix. **Reviews image galleries:** this feature deals with being able to use the selected forensic tool to access and view all images stored which can help a lot in the investigation.

xx. **Easy to install on Windows:** this feature deals with the installation of the forensic tools on Windows (the forensic test environment) without issues.

xxi. **Extract web browser cache history:** The browser's cache history records a user's browsing activity, including the websites visited and the time and date of each visit. This information can be especially valuable for investigators trying to trace a user's online activities and build a timeline of their behavior. As users access websites, the browser generates various types of cache data, such as images and JavaScript files, primarily to improve website loading times. These cache files can serve as a valuable source of information during forensic investigations.

xxii. **Extraction of data from Android smartphones:** this deals with the capability of the forensic tools to extract data from mobile devices as well, thus, helping the forensic investigator to understand the user activity better for the valuable evidence.

xxiii. **Gathering of log files:** Log files are invaluable for post-error forensic investigations, as they allow you to identify the causes of errors or security breaches. These files record data in real time, capturing system activities as they occur. Computer log files supply solid evidence of a user's activity, both online and offline. Event log files are programmatically generated and can be found in operating systems, web browsers, and various computer applications.

xxiv. **Web pages or URL search in a second**: this shows the forensic tool's capability to view several identified web pages or URLs within a second for investigation

xxv. **Deleted files recovery:** this shows the capability of the forensic tool to access the deleted files. Deleted files or hidden data can offer crucial evidence in criminal cases, such as those involving child pornography or murder investigations. This deleted or damaged data may contain key insights and connections that are essential in helping the forensic investigator reveal the truth.

xxvi. **Bookmarking:** Bookmarking is the act of saving and organizing online information for future reference. It can also be a shared activity, enabling users to see how many others have saved the same bookmark and explore related interests. Browser bookmark evidence reveals the information users wanted quick access to or found important and interesting. Additionally, it provides insight into when that information became significant to the user, helping to establish a relevant timeline.

xxvii. **Extraction of cookies:** this is another feature identified by the forensic tool which is a small file situated on a computer's hard drive to keep records. It's being used to conduct various functions, such as recognizing users' subsequent visits to a particular website and tracking the page's visit. Hence, helping the forensic investigator obtain more valuable information about the user's activity.

xxviii. **Perform time zone conversion and selection:** it shows the forensic tool's capability in converting and selecting a particular time zone to work with for the investigation case by the forensic investigator.

xxix. **Presence of thumbnails:** A thumbnail is a small image that represents a larger image, designed to facilitate quicker and easier viewing or management of a group of larger images. Forensic investigators can use the thumbnail cache to identify previously existing pictures within a directory. However, the method of storing and accessing the thumbnail cache can differ depending on the version of Windows being used [31].

xxx. **Generation of QR codes of visited websites:** A quick response (QR) code is a type of barcode that saves information in an arranged set of pixels in a square grid that can be scanned by a digital device. This can be used by the forensic investigator to view and understand information on the websites visited by the user.

xxxi. **Web data extraction:** this deals with various extracted from the websites visited by the user as identified by the forensic tool which can help for further investigation

xxxii. **View of Top Sites (mostly visited sites):** this shows the range of most visited websites by the user which can be helpful in the investigation

xxxiii. **Language options:** these features show the forensic tool's capability of having different language options which the forensic analyst can choose from to have a well-cleared report in a preferred language that is understandable by all.

xxxiv. **SQLite database:** the feature provides controls and wizards that eliminate the need for Structured Query Language (SQL) commands, allowing users to easily generate and develop database files, create and edit tables and indexes, edit and search records, and import or export records and tables as text or CSV files. It maintains a query history for easy revisiting, supports attaching and querying across multiple databases, and keeps a case log of actions. It can help the forensic analyst automatically recover deleted and partial records from databases and associated journals, and it can remove duplicate records if needed.

xxxv. **Lists of connected WLANs:** The forensic tool shows the list of connected Wireless networks that the user used. This can also serve as a piece of valuable evidence if an investigator examines the active status of wireless access points, they can confirm or refute statements based on the information stored in these access points such as a suspect claiming to own only one wireless laptop, then, information can be cross-checked against the records of active wireless access points.

xxxvi. **Lists of connected USBs:** This shows the list of all the connected USB devices to the user's system. It can be found on the File Activity page in which the relevant USB device was selected from the Details column, hence, opening the USB History page, which displays information about the USB device and the events that occurred on it during the currently selected period.

xxxvii. **Mismatch files search:** The Mismatch File Search module examines file contents to identify files whose raw bytes do not align with their file extensions. When it detects discrepancies between extensions and headers, it marks these files accordingly. This allows the examiner to easily identify files with mismatched extensions.

xxxviii. **Create and compare signature:** this deals with comparing the created signature of the identified data to the stored file signature. A file signature helps ensure that the original data stored in a file remains intact and has not been altered. This makes file signatures an essential verification tool, particularly in detecting computer viruses, which digital forensics experts commonly identify.

xxxix. **Indexing:** this deals with the forensic tool creating a catalog by examining an evidence drive and recording the location of each data item. This can help the forensic investigator understand of data arrangement on the suspect device and for proper documentation.

4.2 Evaluation of the identified features for each selected web browser forensic tools

As clearly shown in Table 1, the thirty-nine (39) identified features found in the adopted forensic tools for analysis vary based on the different features each of the forensic tools displayed.

1. **Compatible browsers:** as explained in Table 2, regarding the compatible web browsers for each of the four (5) selected forensic tools used**,** the Browser History Examiner tool (BHE) shows the capability of being compatible with four (browsers) namely: Microsoft Edge, Google Chrome, Internet Explorer and Mozilla Firefox. The Browser History View tool was compatible with all five (5) selected browsers which are Microsoft Edge, Google Chrome, Internet Explorer, Opera Mini, and Mozilla Firefox. The RS Browser tool was also compatible with the five selected browsers while OS forensic tool browsers compatible include Microsoft Edge, Google Chrome, Internet Explorer, and Mozilla Firefox.
2. **Browser settings (profile**)**:** the browser settings profile as explained in section 4.1, was visibly identified in only three (3) forensic tools namely: BHE, BHV, and OS tools.
3. **Export data formats**: The file formats used for generating and exporting reports for BHE and BHV tools are HTML, CSV, and XML. The RS Browser tool exported data formats include HTML, PDF, and Excel while OS Forensic generated report formats are html and pdf.
4. **Login details**: the user's login data stored on the web browsers were easily viewed and extracted by only three forensic tools and these include BHE, RS Browser, and OS forensic tools.
5. **Password recovery:** in the capacity of recovering passwords stored on the browsers by the users, only two forensics tools were identified namely: RS Browser tool (only in a registered version of the tool, that is, a purchased version of the tool) and OS Forensic tool which shows the capability of recovering stored passwords and this can help in investigation by the forensic analyst
6. **Form History:** This feature was identified only in three forensic tools as depicted in Table 1 and these include BHE, RS Browser, and OS forensic tools and

used by the investigator to examine all forms of data users entered into web page forms to track his/her activities

7. **Email messages extraction:** BHE, RS Browser, and OS forensic tools were identified to have the capability of viewing, accessing, and reading all the email messages on the analyzed web browsers which helps in gaining more substantial evidence.
8. **Support Keyword Search:** Table 1 clearly shows that all four (4) forensic tools have the enabling feature of being able to search for some keywords by the forensic analyst while viewing the captured data which helps in obtaining valuable evidence.
9. **Timeline analysis:** the table of the analysis results shows that all four (4) selected forensic tools have the timeline analysis feature which can be used to analyze the set of data points gathered over a specific time interval on the visited websites by the user. This extension enables investigators to track and analyze the user's website usage, providing detailed insights into how much time is spent on each site daily.
10. Extracting artifacts from a web browser: this deals with extracting various data stored by the used web browsers, generally saved in a particular folder within the operating system, hence, serving as a digital clue of the suspect during the investigation.
11. **Hash set filtering:** This filtering process relies on hash calculations. Typically, a hash is computed for each file in the image and compared against a pre-established list of hashes generated from known legitimate files. [32]
12. **Downloads:** The BHE, RS Browser, and OS Forensic tools were able to display the downloads features where all the downloaded files were viewed and contents accessed, hence, providing the digital forensic analyst more insights on the user's activity.
13. **Site storage**: Only BHE and OS forensic tools were clearly shown to have the site storage feature which allows websites to store persistent data (data are consistently fetched by the user on the website) on users' devices, similar to cookies but with a larger capacity and without sending information in HTTP headers. This can also be of great advantage to the forensic investigator in gathering more useful information.
14. **Session tabs**: BHE, RS Browser, and OS forensic tools were identified to display the session tab feature and this can be used by the forensic analyst to track the several session tabs the user opened and closed and the web pages he/she accessed as part of the user's activity.
15. **Favicons:** Only BHE, RS Browser, and OS forensic tools were identified to display the favicons feature which comprised one or more icons associated with a specific website or webpage, helping users quickly identify a website among multiple open tabs or in their browser history. Favicons can also serve as a valuable source of information during forensic investigations, providing additional insight into the websites or locations visited.
16. **Website visits (counts):** All four selected forensic tools (BHE, BHEV, RS browser, and OS forensic tools) were identified to have the "website visits" feature which helps the forensic investigator to understand the number of times the user of the analyzed system visits a particular website.
17. **URL (Uniform Resource Locator) length:** Only the BHV tool was identified to have a URL length feature as it can be of great help to forensic investigators as it can help for easy navigation to various visited websites.
18. **Site setting:** Only BHE and OS forensic tools were discovered to have site setting features in which **e**ach set includes a URL and a Last-Modified timestamp. During testing, URLs were found in these settings that no longer appeared in the standard web history, making this a useful source for uncovering additional evidence for the digital forensic investigator about the websites the user may have interacted with.
19. **Reviews image galleries:** RS Browser and OS forensic tools were identified as having an image gallery review feature to access and view all images stored which can help a lot in the investigation.
20. **Easy to install on Windows:** All four selected forensic tools used for the analysis were easy to install on Windows 10.
21. **Extract web browser cache history:** all four selected forensic tools could extract **web browser cache history.** As users access websites, the browser generates various types of cache data, such as images and JavaScript files, primarily to improve website loading times. These cache files can serve as a valuable source of information during forensic investigations.
22. **Extraction of data from Android smartphones:** RS Browser and OS forensic tools were found to have the capability of extracting information from Android devices that the user might have used or connected to the system for the transfer of some valuable data which can help the forensic analyst during investigation.
23. **Gathering of log files:** All four (4) chosen forensic tools show the list of log files of the used web browsers by the users which can be used for post-error forensic investigations as comprised of real-time data, revealing system activities as they occur.
24. **Web pages or URL search in a second**: all four (4) selected forensic tools comprised of web pages or URL search which was used to search multiple web pages visited by the user.
25. **Deleted files recovery:** This feature was discovered in the RS Browser tool (only in the registered version) and OS forensic tools which were used to already access the deleted files by the user serving as crucial evidence for criminal cases, hence, helping the forensic investigator reveal the truth.
26. **Bookmarking: the** bookmarking feature was found in only BHE, RS Browser, and OS forensic tools which reveals the information users wanted quick access to or found important and interesting. Additionally, it

provides insight into when that information became significant to the user, helping to establish a relevant timeline.

27. **Extraction of cookies: the** cookies extraction feature was found in only BHE, RS Browser, and OS forensic tools which were used to recognize users' subsequent visits to a particular website and track the page's visit. Hence, helping the forensic investigator obtain more valuable information about the user's activity.
28. **Perform time zone conversion and selection:** the time zone conversion and selection for the gathering and creating evidence by the forensic investigator was found in all the selected forensic tools.
29. **Presence of thumbnails:** Only BHE and OS forensic tools show the presence of the thumbnails feature which was used by the Forensic investigator to identify previously existing pictures within a directory
30. **Generation of QR codes of visited websites:** Only BHV forensic tools used the generation of QR codes for each website visited by the user, hence helping the forensic investigator for better view and understanding of information of the websites visited by the user.
31. **Web data extraction:** Only the RS Browser tool was identified to show the web data extraction feature of various visited web pages by the user, helping forensic investigation.
32. **View of Top Sites (mostly visited sites):** Only RS browser and OS forensic tools show the view of top sites (mostly frequently visited websites) by the user which can be helpful in the investigation.
33. **Language options**: Only the RS browser shows various language options specifically eleven (11) different languages including the English language. This also serves as an advantage of helping the forensic investigator to have well-cleared documentation that is understandable by the people or country.
34. **SQLite database:** Only the OS forensic tool shows a visible SQLite database which maintains a query history for easy revisiting, supports attaching and querying across multiple databases, and keeps a case log of actions. It can help the forensic analyst automatically recover deleted and partial records from databases and associated journals, and it can remove duplicate records if needed.
35. **Lists of connected WLANs:** Only the OS forensic tool shows the lists of connected wireless networks of the user's system which can serve as a piece of valuable evidence if an investigator examines the active status of wireless access points, they can confirm or refute statements based on the information stored in these access points such as a suspect claiming to own only one wireless laptop, then, information can be cross-checked against the records of active wireless access points
36. **Lists of connected USBs:** Only the OS forensic tool shows the list of connected USB devices to the user's system. Opening the USB History page helps display information about the USB device and the events that occurred on it during the currently selected period which can help the forensic investigator track and better understand the user's activity.
37. **Mismatch files search:** Only the OS forensic tool was able to show the list of mismatch files search, identifying files whose raw bytes do not align with their file extensions. When it detects discrepancies between extensions and headers, it marks these files accordingly. This allows the examiner to easily identify files with mismatched extensions.
38. **Create and compare signature:** creating and comparing file signature was shown only in OS Forensic helps ensure that the original data stored in a file remains intact and has not been altered. This makes file signatures an essential verification tool, particularly in detecting computer viruses, which digital forensics experts commonly identify.
39. **Indexing:** the indexing feature was found only in the OS forensic tool which helps in creating a catalog by examining an evidence drive and recording the location of each data item. This can help the forensic investigator understand of data arrangement on the suspect device and for proper documentation.

Table 1: The identified valuable features for analyzing web browsers in the selected Forensic tools

FEATURES	BHE	BHV	RS Browser	OS Forensics
Compatible Browsers	Google Chrome, Microsoft Edge, Internet Explorer and Firefox	Google Chrome, Microsoft Edge, Internet Explorer, Firefox, and Opera mini	Google Chrome, Microsoft Edge, Internet Explorer, Firefox and Opera mini	Google Chrome, Microsoft Edge, Internet Explorer, Firefox
Browser settings (profile)	**Yes**	**Yes**	**No**	**Yes**
Export data formats	Html, CSV, and XML	CSV, HTML, and XML	HTML, EXCEL, and PDF	HTML and PDF
Login details	**Yes**	**No**	**Yes**	**Yes**
Password recovery	**No**	**No**	**Yes (only in the registered version)**	**Yes**
Form History	**Yes**	**No**	**Yes**	**Yes**
email messages extraction	**Yes**	**No**	**Yes**	**Yes**
Support Keyword Search	**Yes**	**Yes**	**Yes**	**Yes**
Timeline analysis	**Yes**	**Yes**	**Yes**	**Yes**
Extracting artifacts from a web	**Yes**	**No**	**Yes**	**Yes**

browser				
Hash set filtering	**Yes**	**No**	**No**	**Yes**
Download	**Yes**	**No**	**Yes**	**Yes**
Site storage	**Yes**	**No**	**No**	**Yes**
Session tabs	**Yes**	**No**	**Yes**	**Yes**
Favicons	**Yes**	**No**	**Yes**	**Yes**
Website visits (counts)	**Yes**	**Yes**	**Yes**	**Yes**
URL length	**No**	**Yes**	**No**	**No**
Site settings	**Yes**	**No**	**No**	**Yes**
Reviews image galleries	**No**	**No**	**Yes**	**Yes**
Easy to install on Windows	**Yes**	**Yes**	**Yes**	**Yes**
Extract web browser cache history.	**Yes**	**Yes**	**Yes**	**Yes**
Extraction of data from Android smartphones	**No**	**No**	**Yes**	**Yes**
Gathering of log files	**Yes**	**Yes**	**Yes**	**Yes**
web pages or URL search in a second	Yes	Yes	Yes	Yes
Deleted files recovery	No	No	Yes (Only in the registered version)	Yes
Bookmarking	Yes	No	Yes	Yes
Extraction of cookies	Yes	No	Yes	Yes
Perform time zone conversion and selection	Yes	Yes	Yes	Yes
Presence of thumbnails	Yes	No	No	Yes
QR code of visited websites	**No**	**Yes**	**No**	**No**
Web Data	**No**	**No**	**Yes**	**No**
View of Top Sites (mostly visited sites)	**No**	**No**	**Yes**	**Yes**
Language options	No	No	Yes	No
SQLite database	No	No	Yes	Yes
Lists of connected WLANs	**No**	**No**	**No**	**Yes**
Lists of connected USB	**No**	**No**	**No**	**Yes**
Mismatch files search	**No**	**No**	**No**	**Yes**
Create and compare signatures.	**No**	**No**	**No**	**Yes**
Indexing	**No**	**No**	**No**	**Yes**

4.3 Rating of the identified (valuable) features for web browser analysis in the selected web browser forensic tools

Table 2 illustrates the rating (percentage) of the valuable features discovered in the four (four) Selected web browser forensic tools for the analysis of web browsers used as a forensic investigator to assess the most effective tool of them. The Browser History Examiner (BHE) tool revealed the total number of twenty-four (24) features out of the total number of thirty-nine found features across all the adopted forensic tools, that is, an overall rating of 61.54% capability-based features for web browser analysis when compared to the selected forensic tools. The identified features include compatible browsers (Microsoft Edge, Google Chrome, Internet Explorer, and Mozilla Firefox), Browser settings (profile), Export data formats, Login details, Form History, Email messages extraction, Support Keyword Search, Timeline analysis, Extracting artifacts from a web browser, Hash set filtering, Downloads, Site storage, Session tabs. Favicons, Website visits (counts), site setting, Easy to install on Windows, Extract web browser cache history, Gathering of log files, Web pages or URL search in a second, Bookmarking, extraction of cookies, Perform time zone conversion and selection, and Presence of thumbnails. Hence, this rated result shows the highly effective capability of the forensic tool which can adopted by a forensic expert to perform web browser analysis that can help to produce substantial evidence which are admissible in a court of law. The Browser History View (BHV) tool was able to capture the total number of thirteen (13) valuable features out of the total number of thirty-nine found features which resulted in the overall rating of 33.33% capability-based features when analyzing the captured web browsers. The identified features include compatible browsers (Microsoft Edge, Google Chrome, Internet Explorer, Opera Mini, and Mozilla Firefox), Browser settings (profile), Export data formats, Support Keyword Search, Timeline analysis, and Website visits (counts),.URL (Uniform Resource Locator) length, Site setting, Reviews image galleries, Easy to install on Windows, Extract web browser cache history, Gathering of log files, Web pages or URL search in a second, Perform time zone conversion and selection, and generation of QR codes of visited websites. This shows a low level of the amount of information a forensic expert can obtain when using BHV for web browser analysis.

RS browser tool captured the total number of twenty-eight (28) out of thirty-nine (39) found features, thus, revealing the overall rating of 71.79% capability-based features for web browser analysis. The identified features include compatible browsers (Microsoft Edge, Google Chrome, Internet

Explorer, Opera Mini, and Mozilla Firefox), Export data formats, Login details, Password recovery, Form History, Email messages extraction, Support Keyword Search, Timeline analysis, Extracting artifacts from a web browser, Downloads, Session tabs. Favicons, Website visits (counts), Reviews image galleries, Easy to install on Windows, Extract web browser cache history, Extraction of data from Android smartphones, Gathering of log files, Web pages or URL search in a second, Deleted files recovery, Bookmarking, extraction of cookies, Perform time zone conversion and selection, Web data extraction, View of Top Sites (mostly visited sites), Language options, and SQLite database. This shows that the use of the RS Browser tool can help in gathering a large amount of valuable evidence based on the available features helping a forensic investigator to gain more insight into the suspect (user)'s activity on the seized system to the appropriate law enforcement agency.

Finally, the OS forensic tool proved to be the best out of all the selected tools with an overall rating of 89.74% capability-based features when analyzing the captured web browsers. It captured the total number of thirty-five out (35) of thirty-nine (39) found features across all the forensic tools. The identified features include compatible browsers (Microsoft Edge, Google Chrome, Internet Explorer, and Mozilla Firefox), Browser settings (profile), Export data formats, Login details, Password recovery, Form History, Email messages extraction, Support Keyword Search, Timeline analysis, Extracting artifacts from a web browser, Hash set filtering, Downloads, Site storage, Session tabs. Favicons, Website visits (counts), Site setting, Reviews image galleries, Easy to install on Windows, Extract web browser cache history, Extraction of data from Android smartphones, Gathering of log files, Web pages or URL search in a second, Deleted files recovery, Bookmarking, extraction of cookies, Perform time zone conversion and selection, Presence of thumbnails, View of Top Sites (mostly visited sites), SQLite database., Lists of connected WLANs, Lists of connected USB, Mismatch files search, Create and compare signature, and Indexing. This clearly shows that the use of OS forensic tools can help to obtain more valuable information than all the other three forensic tools, hence, proving its very high capacity and effectiveness in helping forensic investigators to gather in-depth evidence.

Table 2: Rating of the features in the selected web browser forensic tools

Forensic tool	Number of valuable identified features	percentage
BHE	**24**	**61.54%**
BHV	**13**	**33.33%**
RS browser	**28**	**71.79%**
OS Forensic	**35**	**89.74%**

4.4 The most commonly identified features across all selected forensic tools

Performing a general assessment across all the identified features in the selected forensic tools, a total number of ten (10) features were found to be common. These include:

a) **Compatible browsers:** web browser compatibility was discovered in all four (4) selected forensic tools. However, not all the forensic tools captured all five (5) web browsers as BHE OS forensic tools displayed only four web browsers namely: Microsoft Edge, Google Chrome, Mozilla Firefox, and Internet Explorer while BHV and RS browser tools displayed all five (5) selected web browsers (Microsoft Edge, Google Chrome, Mozilla Firefox, Opera min, and Internet Explorer

b) **Export data formats:** The HTML file format was the most common format discovered for exporting generated data across all the forensic tools. Additionally, in BHE and BHV tools, generated data are also exported as CSV (a simple text file format) and XML (a text-based document format) files. The export data formats in the RS browser also include Excel and PDF file formats, while the OS forensic tool exports generated data in PDF file format as well.

c) **Support keyword search:** All the selected forensic tools have the keyword search feature which enables a forensic investigator to easily search and understand some common words which can help in gaining more insight about the user's activity.

d) Time analysis: Analysing the time interval of some specific data about the user's activity such as website visits which can be valuable evidence for forensic analysts. This was discovered across all the selected forensic tools.

e) **Website visits count:** this summarises the number of times the suspect (user) visits a particular website and this feature shows as one of the most common features across all the forensic tools, hence creating substantial evidence.

f) **Easy to install on Windows:** All four selected forensic tools were used due to their compatibility and suitability with the analyzed Windows 10, hence obtaining a comprehensive evaluation result.

g) **Extract web browser cache history:** web browser cache history was obtained across all the forensic tools, and proved useful and valuable to the forensic investigator.

h) **Gathering log files:** various log files were obtained across all the forensic tools as they summarised the user's log of events and activities and were tenable to the forensic investigator as evidence.

i) **Web pages or URL search in a second:** This was found across all the forensic tools helping forensic investigators to view and access various visited websites for obtaining more information.

j) **Perform time zone conversion and selection**: This was found across all the forensic tools as it helps the forensic investigator to easily set time zone as it suits the country and location where the investigation is performed.

4.5 Comparison of evaluation results of the recent existing (benchmark) work with this paper

As expressed in Table 3 of the existing related work of Adamu who evaluated three (3) different forensic tools namely: Autopsy, Browser History Examiner, and NetAnalysis tools in analyzing three (3) selected web browsers which are Mozilla Firefox, Google Chrome and

Internet Explorer. The research work pointed out the Autopsy forensic tool as the best forensic tool among them of which twenty (20) different features were captured across the three adopted forensic tools [33].

Another recent research was conducted using the WEFA (Web Browser Forensic Analyzer) tool to analyze Mozilla Firefox, Google Chrome, Internet Explorer, Opera, and Safari for the main purpose of Social media forensic extraction. The researcher showcased the capabilities and tools utilized in the web browser for reviewing the records [34]**.**

Autopsy, AXIOM, and XRY forensic tools were adopted to analyze Edge, Safari, and Firefox browsers. The evidence extraction was done from smartphones as well as, evaluating the success rates between rooted or jailbroken devices, and the evidence collected from browsers versus applications was conducted [35]**.**

Another research work was done which involved the application **of** FTK and autopsy forensic tools in analyzing Edge, Safari, and Firefox browsers. Artifacts were discovered in cases involving deleted bookmarks and history, Gmail and Yahoo Mail, Facebook chat, and WhatsApp Web chat while Google Chrome was open in both normal and incognito modes, as well as Google and Outlook credentials accessed in incognito mode. The results indicate that FTK outperforms Autopsy in the extraction of evidence using hard disk forensics [36].

This paper's work worked on the evaluation of four (4) different forensic tools namely: BHE, BHV, RS browser, and OS forensic tools using five (5) selected web browsers: Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, and Opera mini. The evaluation performance captured a total number of thirty-nine (39) Features and indicates OS forensic tool as the best of them all as it comprised thirty=five (35) features which can be of great advantage to be used by the forensic investigator in obtaining more, valuable and substantial evidence when performing live-acquisition analysis of system's web browsers.

Table 3: Comparison of the evaluation result with the existing research work

Author (s)	**Forensic tools used**	**List of Web browsers analyzed**	**Evaluation results**
[33]	Autopsy, BHE, and NetAnalysis	Mozilla Firefox, Google Chrome, and Internet Explorer	A total number of 20 features were identified and the assessment of the chosen tools indicates that Autopsy stands out as the best forensic tool among them.
[34]	WEFA (Web Browser Forensic Analyzer	Mozilla Firefox, Google Chrome, Internet Explorer, Opera, and Safari	Social media forensic extraction was conducted. The researcher showcased the capabilities and tools utilized in the web browser for reviewing the records.
[35]	Autopsy, AXIOM, and XRY	Edge, Safari, and Firefox,	Extraction of evidence from smartphones as well as, evaluating the success rates between rooted or jailbroken devices and the evidence obtained from browsers versus applications were conducted.
[36]	FTK and Autopsy	Google Chrome	Artifacts were discovered in cases involving deleted bookmarks and history, Gmail and Yahoo Mail, Facebook chat, and WhatsApp Web chat while Google Chrome was open in both normal and incognito modes, as well as Google and Outlook credentials accessed in incognito mode. The results indicate that FTK outperforms Autopsy in evidence extraction using hard disk forensics.
This paper	BHE. BHV, RS browser and OS forensic tools	Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, and Opera mini	A total number of thirty-nine (39) features were identified. The evaluation performance reveals the OS forensic tool to be the best of them all in terms of the extracted artifacts including the recovery of deleted files and login details.

6. Conclusion and Future Scope

Having performed a comprehensive evaluation of four (4) different forensic tools namely: Browser History Examiner (BHE), Browser History View (BNV), RS browser, and OS (Operating System) forensic tools on the five (5) selected web browsers which are Google Chrome, Edge, Opera mini, Mozilla Firefox and internet explorer, a total number of thirty-nine (39) valuable features were identified which can serve as admissible valuable evidence by the forensic investigator to the court of law of the suspect's activities.

The Browser History Examiner (BHE) tool was shown to identify the total number of twenty-four (24) features out of the total number of thirty-nine found features across all the adopted forensic tools, that is, an overall rating of 61.54% capability-based features for web browser analysis when compared to the selected forensic tools. It was able to analyze only four (4) out of the five (5) selected web browsers on the analyzed Windows system: Microsoft Edge, Google Chrome, Internet Explorer, and Mozilla Firefox.

The Browser History View tool was revealed to capture a total number of thirteen (13) valuable features out of the total number of thirty-nine found features which resulted in the overall rating of 33.33% capability-based features when analyzing the captured web browsers. It shows the ability to analyze all five selected web browsers which include Microsoft Edge, Google Chrome, Internet Explorer, Opera Mini, and Mozilla Firefox.

The RS browser tool was ascertained to capture the total number of twenty-eight (28) out of thirty-nine (39) found features, thus, revealing the overall rating of 71.79% capability-based features for web browser analysis. It also shows the capability of analyzing all five (5) selected web browsers: Microsoft Edge, Google Chrome, Internet Explorer, Opera Mini, and Mozilla Firefox.

Lastly, the OS forensic tool was proven to be the best out of all the selected tools with an overall rating of 89.74% capability-based features when analyzing the captured web browsers. It captured the total number of thirty-five out (35) of thirty-nine (39) found features across all the forensic tools across only four out of the selected web browsers which include Microsoft Edge, Google Chrome, Internet Explorer, and Mozilla Firefox. This shows that OS forensic tools were capable of discovering the highest number of valuable information on the analyzed Windows 10 system but were able to capture four out of the five selected web browsers.

In conclusion, using a live-acquisition method for capturing data on the Windows 10 system, it has been revealed that although the OS forensic tool has the highest rate of the captured features across all the other selected forensic tools, it only has the capability of analyzing four of the five selected web browsers while RS browser which was the second highest in rating, shows the capability of capturing all the five selected web browsers this implies that each of the selected forensic tools has its capability and as well be used in obtaining useful and valuable information which can be presented acceptably within the law sector depending on the set scope (case), the forensic investigator is dealing with.

However, for future work, it is suggested to employ more accessible forensic tools for analyzing different web browsers based on the scope of the required information as well as analyzing other operating systems such as MacOS, as their usage increases daily as well as changes in digital technology, which poses great challenges to the forensic investigator to more new forensic tools in digging up all form of hidden and vital information of any seized system of the suspect on any given case as well as properly utilizing the forensic process in preserving, identifying, analyzing and reporting the given case. Also, other methods of acquiring data on the seized devices can be considered to obtain more accurate results as well as ensure the integrity of the acquired data.

Data Availability
All details about the analyzed web browser data using the selected forensic tools are available at the request.

Conflict of Interest
The author declares that no party has exerted any undue influence on the publication of this work.

Funding Source
None

Authors' Contributions
The author completed the entire work independently.

Acknowledgments
I am deeply grateful to God Almighty. For His divine guidance, which has illuminated my path and inspired this work. I also extend my sincere gratitude to the International Journal of Scientific Research in Computer Science and Engineering for their invaluable feedback and constructive suggestions, which have greatly improved the clarity and impact of my research.

References

[1] F. Carroll, "Human-Browser Interaction: Investigating Whether the Current BrowserApplication's Design Makes Sense for Its Users?," *INTERNATIONAL JOURNAL OF HUMAN-COMPUTER INTERACTION,* pp.**1-12, 2023.**

[2] D. Dissanayaka and D. Wickramasinghe, "Factors Affecting the Selection of Web Browsers by University Students: Special Reference to Rajarata University," *Journal of Information Systems & Information Technology (JISIT),* Vol.**5**, Issue.**2**, pp.**26-42, 2020.**

[3] S. Gusarov, O. Salmanova, O. Prysyazhnyuk, and Y. Shovkun, "Legal Basis for The Activities of Law Enforcement Agencies Under the Legal Regime of Martial Law," *International Journal of Religion,* Vol.**5,** Issue.**3**, pp.**281-287, 2024.**

[4] N. Nelufule, M. Masango, and T. Singano, "The Future of Digital Forensic Investigations: Keeping the Pace with Technological Advancements," in *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, Opatija, Croatia, **2024.**

[5] H. Dubey, S. Bhatt, and L. Neg, "Digital Forensics Techniques and Trends: A Review," *The International Arab Journal of Information Technology,* Vol.**20**, Issue.**4**, pp.**644- 654, 2023.**

[6] Selim and İ. Ali, "The Role of Digital Forensic Analysis in Modern Investigations," *Journal of Emerging Computer Technologies,* Vol.**4**, Issue.**1**, pp.**1-5, 2024.**

[7] N. P. Bhosale, "Evidence Recovery using EnCase and FTK in Forensic Computing Investigation," *International Journal of Scientific Research in Computer Science and Engineering,* Vol.**9**, Issue.**4**, pp.**8-13, 2021.**

[8] Rasool and Z. Jalil, "A Review of Web Browser Forensic Analysis Tools and Techniques," *Researchpedia,* Vol.**1**, Issue.**1**, pp.**15-21, 2020.**

[9] Souley and A. S. Sambo, "A Comparative Performance Analysis of Popular Internet Browsers in Current Web Applications," *African Journal Online,* Vol.**1**, Issue.**1**, pp.**1-7, 2022.**

[10] Mohamed and I. Ismail, "A Performance Comparative on Most Popular Internet Web Browsers," in *4th International Conference on Innovative Data Communication Technology and Application*, UAE, **2022.**

[11] Noland, "Current Challenges of Digital Forensics," *Themis: Research Journal of Justice,* vol. 12, Issue.1, pp.**5-20, 2024.**

[12] D. Salman and E. H.Hasan, "Survey Study of Digital Forensics: Challenges, Applications and Tools," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, Turkey, 2023.

[13] J. V. 9. I. A. C. I. T. A. O. F. E. I. C. I. NIGERIAbyG.V.OBAMANU1, "LEGAL ISSUES AND CHALLENGES IN THE ADMISSIBILITY OF DIGITAL FORENSIC EVIDENCE IN COURTS IN NIGERIA," *African Journal*, vol. 8, Issue 1, pp.**96-109, 2023.**

[14] H. Fakhouri, M. A. Alsharaiah and A. A. Hwaitat, "Overview of Challenges Faced by Digital Forensic," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, Jordan, **2024.**

[15] A.R. Mahlous and H. Mahlous, "Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser," *when International Journal of Intelligent Engineering and Systems*, vol. 13, Issue 6, pp.**294-306, 2020.**

[16] A. Raza, H. T. Mehdi Hussain, M. Zeeshan, M. A. Raja and K.-H. Jung, "Forensic analysis of web browsers lifecycle: A case study," *Journal of Information Security and Applications*, vol. 85, Issue 103839, pp. **1-10, 2024.**

[17] H. Sanghvi, D. Rathod, P. Shukla, R. Shah, and Y. Zala, "Web browser forensics: Mozilla Firefox," *International Journal of Electronic Security and Digital Forensics,* vol. 16, Issue 4, pp. **397-423, 2024.**

[18] K. Hughes, P. Papadopoulos, N. Pitropakis, A. Smales, J. Ahmad and W. J. Buchanan, "Browsers' Private Mode: Is It What We Were Promised?," *Computers,* vol. 10, Issue 165, pp. **1-20, 2021.**

[19] S. Dija, J. Ajana, V. Indu and M. Sabarinath, "Web Browser Forensics for Retrieving Searched Keywords on the Internet," in *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, **2021.**

[20] H. Fayyad-Kazan, S. Kassem-Moussa, H. J. Hejase, and A. J. Hejase, "Forensic analysis of private browsing mechanisms: Tracing Internet activities," *Journal of Forensic Science and Research,* vol. 5, pp. **012-019, 2021**.

[21] G. B. Akintola and P. V. Falade, "Evaluating the Performances of Digital Data Transmission Links on a Client-Server Network Model," *International Journal of Scientific Research in Computer Science and Engineering,* vol. 12, no. Issue 2, pp.**53-66, 2024.**

[22] Oberlo, "Most Popular Web Browsers in 2024," Oberlo, 1 August **2024.**

[23] K. Gautam, A. Verma and A. Vyas, "An Overview of Age Estimation in Forensic Science: Based on Techniques," *International Journal of Scientific Research in Multidisciplinary Studies,* vol. 1, no. Issue 4, pp. **1-11, 2023.**

[24] N. Ivan, B. Felix, I. f. Agatha and A. Joshua, "THE ADVANCED LIVE DIGITAL EVIDENCE ACQUISITION," *Global Scientific Journal,* vol. 12, Issue 2, pp. **287-326, 2024.**

[25] F. Foxton, "Browser History Examiner," Fxoton software, 1 October **2024.**

[26] Nirsoft, "Nirsoft," Nir Softer, 02 October **2024.**

[27] V. R. K. Kolla, "A Comparative Analysis of OS Forensics Tools," *International Journal of Research in IT and Management (IJRIM),* Vol.**12**, Issue.**4**, pp.**1-14, 2022.**

[28] M. Rodriguez, "Exploring the Landscape of Operating System Forensics: An In-Depth Evaluation," *International Journal of Creative Research in Computer Technology and Design,* Vol.**5**, Issue.**5**, pp.**1-13, 2023.**

[29] D. J. Leith, "Web Browser Privacy: What Do Browsers Say When They Phone Home?," *IEEE ACCESS,* Vol.**1**, Issue.**1**, pp.**1-12, 2021.**

[30] P. Chikkagalagali, A. S. Shirodkar, Gauri, Siddharth, and P. Patil, "Scene Understanding in a Web Browser," in *2024 5th International Conference for Emerging Technology (INCET)*, Belgaum, India, **2024.**

[31] Findlay, "A review of thumbnail images artifacts in the Linux desktop and a methodology to add provenance to deleted files, using the thumbnail images artifact in combination with recent files history, and Trash artifacts," *Forensic Science International: Digital Investigation*, Vol.**44**, Issue.**301498**, pp.**1-9, 2023.**

[32] J. Kävrestad, M. B. and N. Clarke, "Autopsy Forensics," in *In: Fundamentals of Digital Forensics*, Cham, Springer, **2024.**

[33] H. Adamu, A. A. Ahmad, A. Hassan and S. B. Gambasha, "Web Browser Forensic Tools: Autopsy, BHE," *International Journal of Research and Innovation in Applied Science (IJRIAS),* Vol.**6**, Issue.**6**, pp.**56-61, 2021.**

[34] K. G. Majeti, Y. S. Sundar, S. S. Ulichi, S. N. Mohanty and S. SV, "Digital Forensic Advanced Evidence Collection and Analysis of Web Browser Activity," *EAI Endorsed Transactions on Scalable Information Systems,* Vol.**1**, Isssue.**1**, pp.**1-8, 2023.**

[35] M. Alotibi, S. Y. Altaleedi, T. Zia and E. U. H. Qazi, "Examining the Behavior of Web Browsers Using Popular Forensic Tools," *International Journal of Digital Crime and Forensics,* Vol.**16**, Issue.**1**, pp.**1-22, 2024.**

[36] H. Sanghvi and D. Rathod, "Google Chrome forensics," *International Journal of Electronic Security and Digital Forensics,* Vol.**15**, Issue.**6**, pp.**591-619, 2023.**

AUTHORS PROFILE

Grace Bunmi Akintola holds a B.Tech in Computer Science with a specialization in Cyber Security from the Federal University of Technology, Minna, Nigeria (2016), and an MSc in Computer Forensics and Cybersecurity from the University of Greenwich, London, UK (2021). These academic achievements have equipped her with a solid foundation in cybersecurity principles, best practices, and forensic methodologies. She is a member of the Nigeria Computer Society (NCS), which represents all IT professionals, interest groups, and stakeholders in Nigeria. Currently, Grace serves as an Assistant Lecturer in the Department of Cyber Security at the Nigerian Defence Academy (NDA) in Kaduna, Nigeria. In this capacity, she is dedicated to educating and mentoring future cybersecurity professionals, promoting cybersecurity awareness, and engaging in research. Her passion for academic excellence is evident in her ongoing pursuit of knowledge and commitment to her students. Grace's research interests include various aspects of cybersecurity, such as network security, forensics, AI security, and penetration testing, alongside her interest in scholarly writing and research.