JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FORENSIC INVESTIGATION OF GOOGLE CHROME BROWSER ARTIFACTS: ANALYSIS, EVIDENTIARY VALUE, AND INDIAN LEGAL FRAMEWORK

Dr.Bandu B. Meshram[1] Dr. Mahaveer Prasad Mali[2] Dr. Manish Kumar [3]

[1] Faculty, CE, DMCE, Airoli , Navi Mumbai-4000708. RS, NIMS, School of Law, NIMS University Rajasthan, Jaipur,(India).Email: bbmeshram.jes@gmail.com
[2]Assistant Professor , NIMS, School of Law. NIMS University Rajasthan, Jaipur,(India), Email:
[3]Head Of Law Department, NIMS, School of Law. NIMS University Rajasthan, Jaipur,(India),

Abstract

This paper presents a focused forensic investigation of Google Chrome browser artifacts, examining their analytical value, evidentiary significance, and legal relevance in India. As browsers serve as the primary interface for online activity, they are also frequent vectors of cyberattacks, making their forensic analysis indispensable in digital investigations. The study begins with an assessment of browser-based threats and vulnerabilities, followed by a systematic exploration of Chrome's storage structures. Key artifacts identified include browsing history, cache, cookies, downloads, saved credentials, autofill entries, and extensions. These artifacts serve as crucial forensic parameters, enabling investigators to reconstruct user activity, detect malicious behavior, and establish reliable timelines of digital events.

In addition to browser artifacts, the study underscores the importance of network forensics. Elements such as firewall logs, Intrusion Prevention System (IPS) alerts, Internet Service Provider (ISP) records, and web server logs are analyzed to provide corroborative evidence. These network-level traces strengthen attribution by linking user activity to attacker infrastructure, validating browser-derived findings, and offering a broader view of cyber incidents.

The research also integrates technical findings with legal frameworks in India. Statutes including the Information Technology Act, 2000 (addressing unauthorized access, identity theft, and obscene content), the Indian Penal Code, 1860, and the Bharatiya Nyaya Sanhita, 2023, are contextualized to show how browser evidence is applied in prosecution. By bridging forensic analysis with statutory provisions, the paper demonstrates the indispensable role of browser and network forensic evidence in cybercrime detection, prosecution, and judicial accountability in India.

Index Terms : Browser Crimes , Browser Forensics, Google Chrome, Cyber Laws,

1.INTRODUCTION

In the digital era, web browsers function as critical gateways for online activity while simultaneously serving as repositories of digital evidence. Google Chrome maintains extensive artifacts such as history logs, downloads, cookies, bookmarks, and cache files at defined system directories. The forensic examination of these artifacts enables the reconstruction of user behavior, identification of cyber-attack vectors, and attribution of malicious

activity to specific actors. Browser exploitation techniques: including phishing, click jacking, drive-by downloads, cross-site scripting, and man-in-the-browser attacks further underscore the browser's dual role as both a facilitator of interaction and an attack surface.

The evidentiary value of Chrome artifacts is significant but their admissibility requires compliance with statutory provisions under the Information Technology Act, 2000, the Indian Penal Code, and the Bharatiya Nyaya Sanhita, 2023, which govern offenses such as data tampering, unauthorized access, and identity theft. This paper is organized into six sections: (i) an introduction to browser-related crimes, (ii) cyber attacks through browsers, (iii) forensic insights into Chrome artifacts, (iv) network and web-based digital footprints, (v) relevant legal frameworks, and (vi) a conclusion emphasizing the role of browser forensics in cybercrime investigation.

Web browsers are now central to digital life and cybercrime investigations. Google Chrome, the most widely used browser, stores valuable artifacts namely history, downloads, bookmarks, cookies, and cache—that reveal user activity and intent. Forensic analysis of these traces helps investigators reconstruct timelines, detect attack methods, and link actions to threat actors. Chrome also presents vulnerabilities exploited in phishing, XSS, MitB, and other attacks.Legal recognition of such evidence requires adherence to the Information Technology Act, 2000, the IPC, and the Bharatiya Nyaya Sanhita, 2023, which address unauthorized access, data tampering, identity theft, and privacy breaches.

This paper is structured in six parts: 1,introduction, ,2 forensic insights into Chrome,3 network/web footprints, 4.legal provisions, and 5 conclusion. Together, they highlight the indispensable role of browser forensics in combating cybercrime.

2.FORENSIC INSIGHTS INTO GOOGLE CHROME

This section explore the artefacts of Google chromes and their importance in digital forensic.

2.1 Representative Block Diagram For Digital Forensic

The environment and connectivity of components is shown in the representative figure 1 as below.

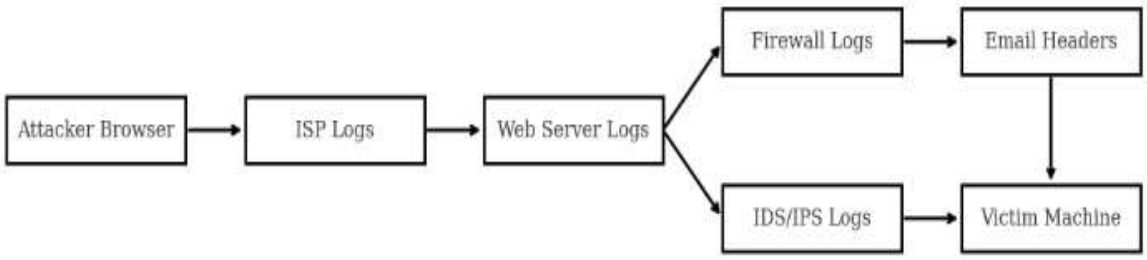

Figure 1. Representative set up for browser forensic

Attack begins with malicious request from attacker's browser which passes through ISP (logs IP, time, route) and reaches web server (HTTP logs, access records) and traffic is filtered by firewall and IDS/IPS (suspicious traffic, alerts) which may then hit victim via phishing/email (headers show sender, path, time). Logs across ISP, server, firewall, IDS/IPS, and email form forensic chain is used to trace attacker-to-victim flow.

2.2 Chrome Artifacts at Attackers Machine

The forensic examination of Google Chrome artifacts Table 3 provides critical insights into user activity and potential cybercrime evidence.

Table 1 Google Chrome Browser Examination Paths[1,2,3,4,5,6].

Artifact Type	Path
History	C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\History (SQLite DB file)
Cache	C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Cache (html, js , image files)
Downloads	C:\Users\<user>\Downloads and browser Download History DB
Cookies	C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Cookies (SQLite)
Bookmarks	C:\Users\(YourUserName)\Local\Google\User Data\Default(JSON file)
Preferences/ Secure Preferences	C:\Users\<Username>\AppData\Local\Google\Chrome\User Data\Default\Preferences C:\Users\<Username>\AppData\Local\Google\Chrome\User Data\Secure Preferences (JSON files)
Extensions	C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Extensions\<extension_id>
DNS Cache	ipconfig /displaydns (CMD)
Packet Captures	.pcap files captured using Wireshark / Fiddler
DevTools .har files	Saved using Network tab → right-click → Save All as HAR

2.3 Artifact Mapping and User Activity in Cybercrime Investigations

In cybercrime forensics, Chrome data at C:\Users<UserName>\AppData\Local\Google\Chrome\User Data\Default holds key evidence. *History, Login Data, Cookies, Cache, Downloads, Bookmarks, Extensions,* and *Web Data* reveal browsing, logins, files, and user interests. Tools like DB Browser, ChromeCacheView, and VS Code (for JSON) extract details; DNS cache, Wireshark, Fiddler, and HAR files provide network evidence. Correlating artifacts builds a timeline, uncovers deleted or encrypted data, and links actions to users or attacks.

Key Data Stored in User Data Folder

The User Data directory contains multiple profiles (like Default, Profile 1, etc.) and each has several files and databases. Important artifacts include:

(a) **History :** The Chrome History file[7], *(Default\History)* is a key forensic artifact stored as a SQLite database. It logs detailed web activity, revealing user behavior and access times to suspicious domains. This helps reconstruct attack timelines and link user actions to threat actors.

Path: *C:\Users\BBM\AppData\Local\Google\Chrome\User Data\History*

Parameters[31, 32] (i) url – Full URL visited (ii) title – Page title (iii) visit_count – Number of times visited (iv) last_visit_time – Timestamp of last visit (Webkit timestamp) (v) typed_count – Number of times typed in address bar (vi) transition_type – Type of navigation (link, typed, bookmark, etc.)

The History file logs visited URLs, access times, visit counts, and typed addresses.

(b) **Cookies** :The Cookies database, found at the path Default\Cookies within the Chrome User Data directory, is another significant source of forensic evidence[8,9,10]

[1] Khan ZH, Naqvi HM, Azeem M, Rauf B. Forensic Analysis of Web Browsers with Emphasis on Google Chrome. International Journal of Computer Science and Network Security. 2020;20(3):67–74.

[2] Sharma A, Kapoor R. Browser Forensics: Identifying and Analyzing Digital Evidence in Web Browsers. International Journal of Computer Applications. 2018;179(31):10–13.

[3] Chand RR, Sharma NA, Kabir MA. Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques. SN Computer Science. 2025;6(1):Article 3921. doi:10.1007/s42979-025-03921-6.ACM Digital Library+1arXiv+1

[4] Bencherchali N. Web browsers forensics. *Medium*. 2018. https://nasbench.medium.com/web-browsers-forensics-7e99940c579a

[5] Foxton Forensics. Google Chrome history location. *Foxton Forensics*.: https://www.foxtonforensics.com/browser-history-examiner/chrome-history-location

[6] Obsidian Forensics. Hindsight: web browser forensics for Google Chrome. *GitHub*.: https://github.com/obsidianforensics/hindsight

[7] Rathod D**.** Web browser forensics: Google Chrome. *Int J Adv Res Comput Sci*. 2017;8(7):896–900. doi:10.26483/ijarcs.v8i7.4433.researchgate.net

[8] Velociraptor Team**.** Windows.Applications.Chrome.Cookies. *Velociraptor Documentation*. [cited 2025 Jun 4]. https://docs.velociraptor.app/artifact_references/pages/windows.applications.chrome.cookies/docs.velociraptor.app

Cookies File Path: C:\Users\<User>\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
The Parameters in Cookies File are (i)host_key: Domain of the cookie (ii)name : Cookie name (iii) value : Cookie value (iv) creation_utc :Timestamp of cookie creation (v)last_access_utc :Last accessed (vi) expires_utc : Expiry
Cookies from attacker-controlled domains can store session IDs, encoded tokens, or IP references that link victim activity to attackers. Set during visits to malicious sites, these cookiesstored at *C:\Users\<UserName>\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies* include fields like domain, name, value, creation time, and expiry, aiding forensic tracing. The cookies *value* field can be particularly important it may include(a) Base64 Tokens: Encoded values (e.g., dmljdGltMTIzNDU2) may reveal usernames, emails, or session IDs, aiding attribution in phishing or tracking cases.(b) Encrypted IP/Fingerprints: Cookies may store encrypted IPs, locations, or device data, enabling cross-session victim tracking and attacker profiling.(c) Tracking Identifiers: Values like 192.168.1.101::session123 link to C2 servers, helping trace victim sessions and attacker infrastructure.(d) Cross-Site Tokens: Shared cookie tokens across domains link multiple sites to one attacker, aiding domain correlation in forensic mapping.Chrome's SQLite cookie file stores cookies, auth tokens, and session IDs; decoding reveals attacker IPs, server links, logins, and user interactions, helping trace hijacked sessions, unauthorized access, and device–web activity in investigations.
(c) Cache : The Chrome Cache folder located at:
C:\Users\<Username>\AppData\Local\Google\Chrome\User Data\Default\Cache
is a vital source of evidence in digital forensic investigations because it stores locally cached web content such as HTML pages, JavaScript files, images, and style sheets retrieved during browsing sessions.
Key Parameters in Cache Files are[11] (i) **url :** The address of the web resource visited (e.g., http://malicious-domain.com/script.js) (ii)data : The actual content of the cached file (e.g., HTML code, JavaScript, embedded images) (iii) timestamp : When the resource was cached, helping determine the timeline of access.
Cached web content is particularly valuable for forensic[12],[13] because (a) Cached files may persist even if the browser history or session data has been deleted by the user or malware.(b) Malicious scripts inspection (e.g., JavaScript or iframe injections) stored in the cache may find /contain hardcoded attacker IP addresses, command-and-control (C2) server URLs, or redirection logic. (c) Investigators can review cached scripts offline for analysis to identify attack mechanisms and trace attacker infrastructure. Example – Realistic Use Case: In a phishing attack investigation[14], a suspect's Chrome cache includes a script named login.js retrieved from http://fakebanking-login.com. On examining the script in the cache:

```
fetch("http://192.168.12.34/exfiltrate.php", {
  method: "POST",
  body: JSON.stringify({ username, password })
});
```

In this example, the IP address 192.168.12.34 is hardcoded into the script, pointing to a data exfiltration endpoint controlled by the attacker. Although this IP may not be visible in browser history or logs, it is preserved in the cached JavaScript file.Furthermore, the timestamp in the cache shows exactly when the script was accessed or executed, helping correlate it with user activity and other system/network logs.
(d). Login Data : The Login Data file (Default\Login Data) is an encrypted SQLite database that stores login credentials saved by users during web browsing protected via Windows DPAPI. In forensics, if decrypted under

[9] Chromium Project**.** sqlite_persistent_cookie_store.cc. Chromium Source Code. https://android.googlesource.com/platform/external/chromium/+/refs/heads/ics-mr0/chrome/browser/net/sqlite_persistent_cookie_store.cc
[10] Morris N, Ahmed U, Patel R. Investigating Google Chrome 66.0.3359 artefact: internet forensics approach. *Int J Comput Sci Mob Comput*. 2018;7(7):112–22.: https://www.researchgate.net/publication/357017151

[11] Khan ZH, Naqvi HM, Azeem M, Rauf B. Forensic Analysis of Web Browsers with Emphasis on Google Chrome: A Case Study. Journal of Information Security and Applications. 2023 May;72:103437. doi:10.1016/j.jisa.2023.103437. https://www.sciencedirect.com/science/article/pii/S2214212623000495
[12] Infosec Institute. Browser forensics: Google Chrome. Infosec Resources.*:* https://www.infosecinstitute.com/resources/digital-forensics/browser-forensics-google-chrome/
[13] SANS Institute. Google Chrome forensics. *SANS Institute Blog*.. https://www.sans.org/blog/google-chrome-forensics/
[14] Tripwire. JavaScript Used by Phishing Page to Steal Magento Credentials. Tripwire. 2021 Mar 4: https://www.tripwire.com/state-of-security/javascript-used-by-phishing-page-to-steal-magento-credentials

the same user profile or with tools, it reveals online credentials, aiding in identifying user behavior, online identities, and tracing unauthorized or malicious activity.

The Login Data file is located at:

C:\Users\<Username>\AppData\Local\Google\Chrome\User Data\Default\Login Data

Structure of the Login Data File :The main table of interest is called **logins**, which includes important fields[15] such as: (i)origin_url: The website URL where the login credentials were saved. (ii) Action_url: The URL where the login form was submitted. (iii)username element: The HTML form element name for the username field. (iv) Username_value: The actual username entered by the user. (v) Password_element: The HTML form element name for the password field. (vi) password_value: The encrypted password. (vii)submit_element: The name of the submit button element on the form. (viii) Signon_realm: The domain associated with the saved credentials.(ix)date_created: The timestamp when the login was saved. (x)blacklisted_by_user**:** Indicates if the user declined to save login for the site. (x) scheme: The authentication method used. (xi) times_used: Number of times the saved credentials have been used.

The Login Data file is forensically significant[16], [17]because The Login Data file is crucial because (a) Chrome passwords are DPAPI-encrypted, needing user access/tools; (b) decrypted logins prove account use, linking suspects to crimes; (c) saved sites show user habits, aiding behavior analysis; (d) mixed legitimate and phishing logins reveal credential theft or compromise; (e) organizational logins expose insider misuse of restricted systems. Example: A corporate data leak investigation uncovered that an employee had saved credentials for restricted internal servers. The Login Data file showed multiple login attempts outside normal working hours, indicating potential insider misuse. These examples highlight how decrypted login data serves as a crucial piece of evidence for establishing identity, reconstructing user activity, detecting breaches, and identifying malicious behavior in cyber forensic investigations.

(e).Web Data: The Web Data file at Default\Web Data stores Chrome autofill entries like names, phones, emails, and partial card details. Though not full payment data, it aids forensics by tracing identity, online behavior, and site interactions, helping profile user habits and personal details for analysis.

The **Web Data** file in Google Chrome is a valuable SQLite database located at:

C:\Users\<Username>\AppData\Local\Google\Chrome\User Data\Default\Web Data

This file stores autofill-related information entered into web forms, and it plays a crucial role in cyber forensic analysis.

Key Parameters (Fields) in the Web Data File

The Web Data file in Chrome maintains several structured tables of user information that are highly relevant in forensic analysis[18]. The autofill table stores form field data, including the field name (e.g., “email” or “first_name”), the corresponding user-entered value, the timestamp of when the data was first created and last used, along with a usage count that indicates how many times the entry was applied. The credit_cards table retains non-sensitive card information such as the cardholder’s name, expiration month and year, and card type (e.g., Visa or MasterCard), while full card numbers are either encrypted elsewhere or stored only with explicit user consent. Complementing these, the autofill_profiles table records detailed user-supplied profile information including full name, email address, company details, postal address, city, state, zip code, country code, and phone number, along with the date the profile was last modified. The Web Data file aids user attribution (autofill values linking activity to individuals), behavioral profiling [19] (types of forms filled), temporal analysis (timestamps of

[15] Ahmad I, Rahman MM, Islam MR, Karim R. Password Recovery from Encrypted Browser Data Using Windows DPAPI: A Forensic Approach. Journal of Digital Forensics, Security and Law. 2023;18(1):45-60. Available from: https://commons.erau.edu/jdfsl/vol18/iss1/5/

[16] Khan ZH, Naqvi HM, Azeem M, Rauf B. Forensic Analysis of Web Browsers with Emphasis on Google Chrome: A Case Study. Journal of Information Security and Applications. 2023 May;72:103437.doi:10.1016/j.jisa.2023.103437.: https://www.sciencedirect.com/science/article/pii/S2214212623000495

[17] Palmenas. Forensic Recovery of Chrome Based Browser Passwords [Internet]. Medium. 2023 Jan 15: https://palmenas.medium.com/forensic-recovery-of-chrome-based-browser-passwords-e8df90d4a3cd

[18] Khan ZH, Naqvi HM, Azeem M, Rauf B. Forensic Analysis of Web Browsers with Emphasis on Google Chrome: A Case Study. Journal of Information Security and Applications. 2023 May;72:103437. doi:10.1016/j.jisa.2023.103437. Available from: https://www.sciencedirect.com/science/article/pii/S2214212623000495

[19] Abdelnabi M, Elhoseny M, Hegazy O, Hassanien AE. Browser Forensics and User Behaviour Analysis: A Survey. Journal of Information Security and Applications. 2022 Apr;61:102918. doi:10.1016/j.jisa.2021.102918. Available from: https://www.sciencedirect.com/science/article/pii/S2214212621003192

interactions), cross-artifact correlation (with history, logins, cookies), and identity verification (supporting or challenging claimed identities), making it crucial in digital forensics.

(f) Bookmarks : The Bookmarks file, located at Default\Bookmarks, is a JSON file that contains a list of websites saved by the user in the Chrome browser.

Bookmarks File: The Bookmarks file in Google Chrome is located at:

Path: C:\Users\<User>\AppData\Local\Google\Chrome\User Data\Default\Bookmarks

Parameters are name : Bookmark name , url : Bookmark URL and date_added: When the bookmark was created.This file stores all user-saved URLs and folders in JSON format. Each entry contains metadata such as the URL, title, date added, and folder structure. Although bookmarks are typically user-driven and static, in forensic investigations, their relevance becomes significant when they include links to phishing sites or attacker-controlled Command-and-Control (C2) domains.

Bookmarks reveal persistence of malicious intent (saved phishing pages), C2 endpoints (links to Remote Access Trojan, /malware panels), social engineering traces (fraudulent login/update pages), timeline evidence (date_added field correlation), and threat intelligence links (cross-check with feeds), making them critical in digital forensics infrastructure.

Example (from Bookmarks file):

```
{
  "date_added": "13320478909876543",   "id": "5",   "name": "Admin Login",
  "type": "url",   "url": "http://malicious-login[.]xyz"
}
```

In this example, the user has bookmarked a login page hosted on a suspicious domain. This may indicate interaction with a fake or cloned site, often used in credential harvesting campaigns.

Thus, bookmarks may reveal deliberate or manipulated engagement with attacker infrastructure and serve as evidence of phishing exposure or use of a system to manage or communicate with C2 servers. Analyzing these entries contributes to understanding the scope, tactics, and timeline of the cyberattack.

(f) Downloads : The Downloads history[20] is stored within the same Default\History SQLite database used by the Chrome browser to track browsing activity. The Downloads artifact in Google Chrome, typically stored in the History SQLite database at C:\Users<UserName>\AppData\Local\Google\Chrome\User Data\Default\History, contains a table named downloads or downloads_url_chains that tracks files downloaded through the browser. The key parameters include (i) target_path : the location where the file was saved, (ii) tab_url : the source URL of the download, (iii) start_time : when the download began, (iv) end_time : when the download ended, (v) received_bytes : the total size of the file, and (vi) danger_type : which indicates if the file is malicious or suspicious. Along with these parameters, additional metadata is recorded such as (vii) the download URL, (viii) file name and saved path, (ix) file size, (x) MIME type, (xi) start and end timestamps, (xii) referrer URL, (xiii) total bytes downloaded, and (xiv) the status of the download, whether completed, interrupted, or flagged as dangerous.This artifact becomes forensically significant when attackers use social engineering or malicious websites to trick users into downloading files that are, in fact, malware, remote access trojans (RATs), keyloggers, or backdoors**.** The actual file saved on disk will usually be in:C:\Users\<Username>\Downloads\

Timestamp: 2025-06-10 14:22:41 ,File Name: updateTool.exe ,URL: http://securebanking-updates[.]com/updateTool.exe ,Browser: Google Chrome ,Download Path: C:\Users\victim\Downloads\updateTool.exe ,File Hash (SHA256): 9f2b1a6d3e4c98f7d7a4c92e01a8e45d3c5a0f8c6fbc2e1d8c4c1baf9e93c12d

Forensic Finding: File identified as Remote Access Trojan (RAT),C2 Communication: 185.243.10.22

A user visits a phishing site pretending to be a bank's security portal. The site tricks the user into downloading updateTool.exe, claiming it is required for enhanced security. This file is logged in Chrome's downloads table

[20] Ibrahim S, Al Herami N, Al Naqbi E, Aldwairi M. Detection and Analysis of Drive-by Downloads and Malicious Websites. In: Proceedings of the 2020 IEEE International Conference on Computer Communications and Networks (ICCCN); 2020 Jul 6–9; Virtual Conference. IEEE; 2020. p. 1–8. doi:10.1109/ICCCN49295.2020.9209652. Available from: https://ieeexplore.ieee.org/document/9209652

with the URL http://securebanking-updates[.]com/updateTool.exe. Forensic analysis later reveals the file is a known RAT communicating with a C2 server at 185.243.10.22.

Download records log filenames, URLs, and timestamps, helping investigators trace suspicious files, identify malicious or illegal content, and reconstruct user actions for case relevance.

7.Extensions / Plugins :The Extensions folder**,** located at Windows C:\Users\<Username>\AppData\Local\Google\Chrome\User Data\Default\Extensions\ , contains data related to the browser extensions and plugins installed in the Chrome browser. These extensions can significantly alter browser functionality, and in some cases, may include malicious or privacy-invasive tools used for activities such as data collection, surveillance, or unauthorized access. In cyber forensic investigations, analyzing installed extensions helps identify suspicious or harmful add-ons**,** detect potential security breaches**,** and understand how the browser may have been used to carry out or facilitate cybercriminal activities**.**

3. NETWORK & WEB BASED SYSTEM ARTIFACTS

The following sections explain how digital forensic experts utilize this information during investigations

3.1 Firewall Logs

Firewall logs[21],[22] capture key details for tracing attacker activity: (i) timestamp: exact event time, (ii) source IP: origin address, (iii) destination IP: target system, (iv) source port: origin port, (v) destination port: targeted service, (vi) protocol: TCP/UDP/ICMP, (vii) action: allowed or blocked. Firewall logs help identify attacker IPs (repeated or unusual connections on vulnerable ports), support timeline reconstruction (aligning events with browser artifacts), enable correlation (e.g., cache file and malicious IP match), reveal attack nature (brute force, callbacks, exploitation by port/protocol), and show defense status (blocked vs allowed traffic indicating protection or misconfiguration).

Forensic Use Case: A corporate system is suspected to be part of a data breach. Firewall logs show the following repeated pattern:

Timestamp: 2025-06-01 03:02:18 ,Source IP: 185.203.119.12 ,Destination IP: 10.0.0.15
Source Port: 54566 ,Destination Port: 3389 ,Protocol: TCP ,Action: Allowed.

This record shows that On 2025-06-01 at 03:02:18, firewall logs show external IP 185.203.119.12 connecting via TCP port 3389 (RDP) to internal host 10.0.0.15, action allowed—indicating possible remote access and potential breach entry point.This entry strongly suggests that the attacker successfully reached the internal system's RDP service, potentially serving as the entry point for the suspected data breach.

3.2 IDS/IPS LOGS

Intrusion Detection System (IDS**)** and Intrusion Prevention System (IPS) logs play a pivotal role in cyber forensic analysis, especially in identifying and attributing attacker activities to specific IP addresses[23],[24] . The key parameters in IDS/IPS logs include (i) timestamp, which indicates when the intrusion or anomaly was detected; (ii) source IP, representing the IP address initiating the suspicious activity (potential attacker); (iii) destination IP, referring to the targeted system or server under attack; (iv) signature_id, a unique identifier of the attack pattern or rule triggered; and (v) threat_type, which specifies the category of the detected attack (e.g., SQL injection, port scan, malware).

.**Example ForensicIDS/IPS lOG:** An organization notices abnormal traffic and checks its IDS logs:

Timestamp: 2025-06-01 04:02:41 ,Source IP: 185.199.109.77 ,Destination IP: 192.168.0.21

[21] Shafiq M, Liyanage M, Ylianttila M. Blockchain and Fog Computing for Secure Firewall and Intrusion Detection Systems in 5G Networks. IEEE Communications Magazine. 2023 Mar;61(3):50-56. doi:10.1109/MCOM.001.2200227. Available from: https://ieeexplore.ieee.org/document/9944462

[22] Singh A, Chatterjee S, Kim D. Firewall Log Analysis for Intrusion Detection using Machine Learning Techniques. Journal of Network and Computer Applications. 2024 Jan;208:103494. doi:10.1016/j.jnca.2023.103494. https://www.sciencedirect.com/science/article/pii/s1084804523002359

[23] Zhang Y, Li Z, Wang C, Xu J. Deep Learning-Based Intrusion Detection Using Hybrid Features in Network Security. IEEE Transactions on Network and Service Management. 2023 Feb;20(1):387-399. doi:10.1109/TNSM.2022.3218301. Available from: https://ieeexplore.ieee.org/document/9734051

[24] Aljawarneh S, Aldwairi M, Yassein M. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Information Security and Applications. 2021 Feb;57:102620. doi:10.1016/j.jisa.2020.102620. Available from: https://www.sciencedirect.com/science/article/pii/S2214212620304056

Signature_ID: 2002857 ,Threat Type: Remote Code Execution – Log4j CVE-2021-44228

From this log, a digital forensic investigator would understand that at 04:02:41 on 1 June 2025, a system with source IP 185.199.109.77 (external attacker) attempted to exploit the internal host 192.168.0.21 (target system) using a Remote Code Execution attack linked to Log4j vulnerability (CVE-2021-44228). The signature_ID 2002857 confirms that the IDS detected a rule specifically mapped to this critical exploit.

3.3 Web Server Logs

Web server logs record all HTTP/HTTPS requests with key metadata, serving as crucial forensic evidence to trace and identify malicious actors during probes or attacks. Apache Web Server, the logs that contain these key parameters are usually:(i)access.log : Records all client requests (contains timestamp, client IP, requested URI, user-agent, referer). (ii)error.log : Records server-side errors, warnings, and diagnostic information.

The key parameters in web server logs include (i) timestamp: exact date and time of the request, (ii) client IP: address of the requesting user or attacker, (iii) requested URI: resource accessed such as login page, admin panel, or vulnerable script, (iv) user-agent: client software used like browser, bot, or attack tool, and (v) referer: previous webpage from which the request originated, helping trace navigation paths.

Apache Web Server Log Entry:

192.0.2.33 - - [02/Jun/2025:02:30:25 +0000] "GET /admin HTTP/1.1" 401 528 "-" "sqlmap/1.5.2#stable"

Where Forensic Interpretation:(i) Client IP: 192.0.2.33, identified as suspicious, (ii) URI: /admin, a restricted page targeted, (iii) User-Agent: sqlmap, confirming use of an automated SQL injection tool, (iv) this single entry demonstrates an attempted unauthorized access using automation, and (v) correlation of the same IP across IDS logs or Chrome cache artifacts further strengthens attribution to the attacker.

3.4 ISP Logs

Structure of ISP Logs: Internet Service Providers (ISPs) maintain various types of logs for regulatory compliance, network management, and law enforcement requests. These logs are not always standardized, but they typically include[25],[26],[27]:

a).Subscriber Information Logs Logs record the (i) Subscriber Name(ii)Installation Address (iii)Billing Address (iv)Registered Phone/Email (v) Customer Account Number (vi)MAC Address (Router/Device) (vii)Static/Dynamic IP Assignment (viii)Registration and Deactivation Dates

b). IP Assignment Logs record the (i) Timestamp (Start and End Time) (ii) Public IP Assigned (iii) Customer Account/Session ID (iv) MAC Address or CPE Identifier (v) Port Number in NAT or CG-NAT scenarios.

c). Connection Session Logs record the (i) Session Start and End Time (ii) User Login (if applicable) (iii) IP Address Used (iv) Bandwidth Consumed (v) Traffic Metadata including destination domains and protocol types.

d). DNS Query Logs record the (i) Timestamp (ii) Client IP (user) (iii) Queried Domain Name (iv) Resolved IP Address (v) Query Type such as A, AAAA, MX, etc.

e). Email/SMTP Logs record the (i) Sender and Recipient Addresses (ii) Timestamp (iii) Subject Line where available (iv) IP of Sender (v) Delivery Status and Server Logs.

a) Subscriber Information Logs

Subscriber Name	Installation Address	Billing Address	Registered Phone/Email	Account No.	MAC Address	IP Assignment	Registration Date	Deactivation Date
Jeman Meshram	Flat 2/2, Greenhouse, Mum	Same as Installation	9876043410 / jeman@gmail.com	CUST345	00:1A:2B:3C:4D:5E	Dynamic	2022-03-10	Active

[25] Kumar A, Singh R, Verma A. Role of ISP Logs in Cybercrime Investigation: A Review. *International Journal of Cyber Security and Digital Forensics*. 2023;12(1):35–42. https://doi.org/10.34105/ijcsdf.2023.12.004.

[26] Singh P, Sharma S. Forensic Analysis of ISP Data in Identifying Cyber Attackers: Recent Trends. *Journal of Digital Forensics, Security and Law*. 2024;19(2):57–68. https://doi.org/10.15394/jdfsl.2024.1765

[27] European Union Agency for Cybersecurity (ENISA). Best Practices for Forensic Readiness and Investigation of ISP Logs. ENISA Report. 2023. Available from: https://www.enisa.europa.eu/publications/forensic-readiness-isp-logs

	bai							

b) IP Assignment Logs

Timestamp Start	Timestamp End	Public IP Assigned	Account No.	MAC/CPE ID	NAT Port
2025-08-25 10:15:00	2025-08-25 11:05:00	103.25.88.112	CUST345	00:1A:2B:3C:4D:5E	45023
2025-08-25 11:05:01	2025-08-25 12:45:00	103.25.88.113	CUST345	00:1A:2B:3C:4D:5E	45024

c) Connection Session Logs

Session Start	Session End	User Login (if any)	IP Address Used	Bandwidth Consumed	Traffic Metadata (Domains / Protocols)
2025-08-25 10:15:00	2025-08-25 11:05:00	rahul123	103.25.88.112	1.2 GB	www.youtube.com (HTTPS), smtp.gmail.com (SMTP), www.tribunal.gov.in (HTTPS)

d) DNS Query Logs

Timestamp	Client IP	Queried Domain	Resolved IP	Query Type
2025-08-25 10:16:10	103.25.88.112	www.youtube.com	142.250.193.238	A
2025-08-25 10:16:11	103.25.88.112	smtp.gmail.com	142.250.150.108	MX
2025-08-25 10:17:45	103.25.88.112	www.tribunal.gov.in	164.100.94.36	A

e) Email/SMTP Logs

Timestamp	Sender Address	Recipient Address	Subject	Sender IP	Delivery Status
2025-08-25 10:18:20	jeman@gmail.com	office@company.com	Meeting Update	103.25.88.112	Delivered
2025-08-25 10:19:05	jeman@gmail.com	friend@yahoo.com	Party Photos	103.25.88.112	Deliver

This type of integrated ISP record allows investigators, regulators, or network admins to trace:
If investigators find suspicious activity from IP 103.25.88.112 at 10:16 AM on 25th August 2025, they can reconstruct: (i)Who: Jeman Meshram (subscriber info) (ii)When: 10:15–11:05 AM (session log) (iii)Which IP: 103.25.88.112 assigned to jeman at that time (assignment log) (iv)What activity: Accessed YouTube, Gmail SMTP, and tribunal.gov.in; sent an email titled "Meeting Update" (DNS + session + email logs)

3.6 Email Headers in Digital Forensics

In digital forensics, email and browsers are closely linked, as browsers often manage webmail accounts[28],[29],[30] Browser artifacts—history, cache, cookies, autofill—show webmail use; stored credentials reveal accounts or logins; attachments/downloads leave URL, time, and action metadata; session cookies/tokens expose active sessions; email header links trace phishing. Analyzing browser and email artifacts together strengthens forensics by correlating access, sharing, and user intent.

Example: Gmail Webmail Server Log

Jun 02 11:25:45 mail.gmail.com smtpd[2456]: 9ABCD12345: client=203.0.113.55[203.0.113.55]
Jun 02 11:25:46 mail.gmail.com cleanup[2460]: 9ABCD12345: message-id=<attacker@evilmail.com>
Jun 02 11:25:47 mail.gmail.com qmgr[2462]: 9ABCD12345: from=<attacker@evilmail.com>, size=3080, nrcpt=1 (queue active)

[28] RFC 5321. Simple Mail Transfer Protocol. IETF; 2008.: https://www.rfc-editor.org/rfc/rfc5321
[29] Cyber 5W. Email Forensics :Expert DigitalForensics Training& Consulting: https://cyber5w.com/
[30] Cado Security. Email Forensics: How to Investigate Digital Communication 2025 Jan 10 Available from: https://www.cadosecurity.com/blog/email-forensics-how-to-investigate-digital-communicationcadosecurity.com

Jun 02 11:25:49 mail.gmail.com smtp[2465]: 9ABCD12345: to=<victim@gmail.com>, relay=mx.gmail.com[74.125.140.27]:25, status=sent (250 2.0.0 OK)

In a webmail server log, (i) timestamp Jun 02 11:25:45 shows when Gmail processed the email, useful for aligning with artifacts; (ii) queue ID/message ID 9ABCD12345 and <attacker@evilmail.com> uniquely identify the mail, enabling trace across servers; (iii) source IP 203.0.113.55 reveals the client submitting the mail, aiding attacker attribution; (iv) sender address (MAIL FROM) <attacker@evilmail.com> is the claimed origin, requiring SPF/DKIM validation; (v) recipient address (RCPT TO) <victim@gmail.com> confirms the attack target; (vi) SMTP status code 250 2.0.0 OK verifies Gmail accepted and delivered the mail; and (vii) relay/delivery info mx.gmail.com[74.125.140.27]:25 records the handling server, proving delivery path and network hops.

This log confirms that an email claiming to be from <attacker@evilmail.com> was sent from IP 203.0.113.55, processed by Gmail, and successfully delivered to <victim@gmail.com>. Using the timestamp**,** Message-ID**,** and Source IP, investigators can correlate with firewall, IDS, browser history, or endpoint artifacts to prove phishing/malware delivery.

3.7 Correlation Process to Identify Attacker's IP Address

Tracing an attacker's IP relies on correlating browser artifacts, network logs, and server/email records, linking victim activity to attacker infrastructure for attribution[31],[32].[33] .

Step 1: Extract timestamps from Chrome history, which logs visited URLs with exact times; investigators identify access to suspicious domains to establish a temporal anchor for correlation. correlation[34].

Case Study: *During the investigation of a corporate breach, Chrome history revealed that an employee accessed* malicious-domain.xyz *at 11:03:24 AM on May 15, 2025. This timestamp became crucial for aligning other data points.*

Step 2: Check Downloads : Next, analysts check download logs from the same period to see if malicious files were fetched; entries with file names and source URLs are cross-referenced with browsing history to confirm links to the suspicious site.

Case Study: *At around 11:03:26 AM, a file named* invoice_update.exe was downloaded from *malicious-domain.xyz*. This download coincided closely with the visit to the site, suggesting a possible infection vector.

Step 3: Inspect Cookies and Cache: Next, analysts review cookies from the suspicious domain for session tokens or attacker links and examine cached JavaScript for hardcoded C2 server IPs used for persistent control.

Case Study: *Analysts found a cookie from* malicious-domain.xyz *with encoded session data time stamped 11:03:24 AM. Cache analysis uncovered JavaScript containing a hardcoded IP,* 185.216.140.99*, suspected to be the attacker's C2 server.*

Step 4: Match Timestamps with Network Logs (Firewall/IDS): The next phase involves correlating browser activity timestamps with network traffic logs[35]. Firewalls and Intrusion Detection Systems (IDS) provide records of outbound connections from the victim's machine. An investigator look for connections initiated at the same time as the suspicious browsing or downloads, focusing on destination IPs contacted during these windows.

Case Study: *Firewall logs recorded an outbound connection from the victim's workstation at 11:03:25 AM, immediately after the malicious download. The destination IP matched the one found in cached scripts:* 185.216.140.99 *on port 443.*

*Step 5: Trace in Firewall/IDS Logs :*Detailed examination of firewall [36] and IDS logs confirm victim–attacker communication, showing source and destination IPs, ports, protocols, and whether connections were allowed or blocked.

---

[31] European Union Agency for Cyber security (ENISA). Forensic Correlation Techniques for Network and Endpoint Logs. ENISA Report. 2023. Available from: https://www.enisa.europa.eu/publications/forensic-correlation-techniques

[32] Awoyemi JT, Jawalekar PS, Keerthika A. A Survey on Browser Forensics: Analysis of Digital Evidence from Web Browsers. ACM Computing Surveys. 2023;55(4):1-29. doi:10.1145/3570043

[33] Singh P, Sharma S. Correlating Multi-Source Logs for Accurate Attacker IP Identification. *Journal of Digital Forensics, Security and Law*. 2024;19(3):78–89. https://doi.org/10.15394/jdfsl.2024.1802

[35] Kumar A, Singh R, Verma A. Role of Browser Artifacts and Network Logs in Cyber Attack Attribution. *International Journal of Cyber Security and Digital Forensics*. 2024;13(1):21–30. https://doi.org/10.34105/ijcsdf.2024.13.003

[36] Gupta M, Reddy B. Practical Approaches to Mapping Browser Artifacts with Firewall Logs in Cybercrime Investigations. *Cyberlaw Journal*. 2023;16(2):99–108.

Case Study: Firewall log entry showed the victim's IP connecting to 185.216.140.99 over port 443, with the action marked as "allowed." IDS logs also flagged this connection as suspicious but permitted it due to encrypted HTTPS traffic.

Step 6: Validate via Server Logs and Email Headers: Finally, server logs and email headers provide external validation. If phishing was involved, email headers often contain X-Originating-IP fields showing the sender's IP address. When this IP matches those identified in firewall and browser cache analyses, the attribution to the attacker's infrastructure is strengthened.

Case Study: *Email headers from a phishing message received by the victim revealed an originating IP of* 185.216.140.99. *The recurrence of this IP across browser cache, network logs, and email headers confirmed it as the attacker's address.*

Summary of Case Outcome:

- Malicious Domain Visited**:** *malicious-domain.xyz*
- Visit Time**:** 2025-05-15 11:03:24
- Cookie Set By Domain**:** *malicious-domain.xyz* at the same time
- Downloaded File**:** *invoice_update.exe* at 11:03:26
- Firewall Outbound Connection**:** Destination IP *185.216.140.99*, port 443, at 11:03:25, action allowed
- Email Header X-Originating-IP**:** *185.216.140.99*

Attacker IP Identified: 185.216.140.99

This comprehensive correlation process demonstrates how combining multiple forensic artifacts across different layers of the digital environment can pinpoint the attacker's IP address with high confidence, enabling precise threat attribution and supporting legal prosecution or remediation.

4.LEGAL PROVISIONS USED IN BROWSER FORENSICS

Legal provisions used in browser forensics involve the Information Technology Act(IT), 2000 for cyber offences, along with the Indian Penal Code(IPC), 1860 / Bharatiya Nyaya Sanhita(BNS), 2023 for cheating, fraud, obscenity, and criminal conspiracy traced through browser activity. Additionally, the Indian Evidence Act(IEA), 1872 / Bharatiya Sakshya Adhiniyam(BSA), 2023 governs the admissibility and certification of browser artifacts as electronic evidence in court.

4.1 IT Act, 2000

This section identify the most key sections used in browser forensic[37]

(i)Section 43 Unauthorized Access and Data Theft: Section 43 on unauthorized access and data theft applies in browser forensics when browsers are used to access restricted sites or extract sensitive data; investigators use history, cache, cookies, and downloads to trace and prove such activity.

(ii) **Section 66 Computer-Related Offences**In browser forensics, this section applies when patterns show attempts to access restricted systems, manipulate data, or act dishonestly; repeated URLs, unusual bookmarks, and cached artifacts evidence the mens rea.

(iii) **Section 66C Identity Theft:** This section applies in cases where browser-stored passwords, cookies, or session tokens are misused for unauthorized access to someone else's digital identity; forensic analysis of saved login credentials and autofill data in browsers helps prove identity theft and link it directly to the suspect.

(iv) **Section 66D Cheating by Personation (Online):** Browser forensics is crucial when saved sessions, autofill data, or login credentials are used by a person to impersonate someone else online and commit fraud; artifacts such as browsing history, session files, and credential storage provide clear digital evidence of online personation.

(v) **Section 67 Publishing or Transmitting Obscene Content:** This section is applied when forensic investigation of a browser reveals history, bookmarks, downloads, or cache files showing access to, transmission, or distribution of obscene and explicit digital content; such artifacts can be used to prove violations under this section.

(vi) **Section 69 Government Powers of Decryption:** In browser forensics, this section empowers authorized agencies to lawfully extract and decrypt encrypted browser data such as login databases, cookies, saved

[37] Information Technology Act, 2000 **:**Government of India. *Information Technology Act, 2000*.]. New Delhi: Ministry of Law, Justice and Company Affairs; 2000 https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

passwords, and browsing sessions; forensic tools used under proper authorization allow investigators to access otherwise hidden or protected digital evidence.

4.2 Addressing Browser-Based Cyber Attacks under IPC 1860 and BNS 2023

This section identify the key sections which can be used in browser forensic cases[38],[39],[40]

4.2.1 Browser-Based Cyber Attacks under IPC 1860

(i) **Section 378 and 379 of IPC : Theft and Punishment for Theft:** Under these sections of the Indian Penal Code, stealing any form of property, including digital data, is considered a crime. If a forensic expert finds that someone has downloaded or transferred confidential files or data using a browser (e.g., through downloads or online file sharing tools), this data theft is treated as a punishable offense. The forensic report helps prove that theft was done using a specific user's browser.

(ii) **Section 403 of IPC : Dishonest Misappropriation of Property**: This section punishes someone who dishonestly misuses property or information that they had access to legally. In browser forensics, if a person uses their access to a shared or office computer to visit private links or download files for personal gain without permission, it amounts to misappropriation. Evidence such as bookmarks or history logs can show this misuse.

(iii) **Section 406 and 409 of IPC – Criminal Breach of Trust:** These sections deal with the criminal offense of breaking someone's trust by misusing assets entrusted to them. If someone entrusted with access to sensitive systems uses the web browser to copy or leak confidential information, browser forensic data like history, downloads, or extensions can help prove this breach of trust. Section 409 is stricter and applies if the offender is a public servant or works in a position of responsibility.

(iv) **Section 419 and 420 of IPC – Cheating and Personation :**These sections punish cheating and impersonating another person to commit fraud. If someone uses saved credentials or web sessions from another person's browser to log into websites and perform fake transactions or send misleading emails, forensic examination of browser history and session tokens can be used as evidence. Tools can recover saved usernames, access patterns, and cookies to prove the fraud.

(v) **Section 468 of IPC – Forgery for the Purpose of Cheating :** This section applies when digital forgeries are made with the intention of cheating. If browser plugins or visited sites indicate the use of tools to generate fake documents, identities, or signatures, then this section can be invoked. Browser forensics can uncover use of such tools or sites, and downloaded fake files can be strong evidence of forgery.

4.2.2 Browser-Based Cyber Attacks under BNS, 2023

(i) Section 68 of BNS, 2023 – Cheating by Personation Through Electronic Means :This newly formulated section under BNS deals specifically with personation using digital tools. It applies when someone cheats others by pretending to be someone else online. Forensic experts use browser data such as login sessions, cookies, and autofill details to show that the accused impersonated someone electronically and accessed digital accounts or services unlawfully.

(ii) Section 69 of BNS, 2023 – Identity Fraud Using Digital Credentials :This section is aimed at controlling the misuse of digital identity like login passwords, biometric tokens, or saved credentials. In browser forensic investigations, this section is used if Chrome's Login Data file or cookies reveal that someone used another person's identity to gain access to services. It supports prosecution by proving digital impersonation with browser-based evidence.

(iii) Section 73 and 74 of BNS, 2023 Cyber Trespass and Data Theft: These newly defined sections cover unauthorized digital access (cyber trespass) and stealing of electronic data. Browser forensic tools often uncover such activity when the history shows entry into secure systems, or downloads include sensitive files without permission. Extensions or plugins used to bypass security can also be tracked to prove data theft and unauthorized access.

(iv) Section 122 of BNS, 2023 Criminal Breach of Trust by Electronic Means :This section punishes individuals who misuse digital platforms to break the trust of organizations or individuals. In the context of browser forensics, it

[38] Indian Penal Code, 1860 **:**Government of India. *The Indian Penal Code, 1860*. New Delhi: Ministry of Law and Justice; 1860: https://www.indiacode.nic.in/handle/123456789/2263

[39] Bharatiya Nyaya Sanhita, 2023 :Government of India. *The Bharatiya Nyaya Sanhita, 2023*. New Delhi: Ministry of Home Affairs; 2023: https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

[40] Singh A, Verma P. AI-Powered Cybercrime Investigations under BNS. *International Journal of Law Management & Humanities* 2023 https://ijlmh.com/wp-content/uploads/AI-Powered-Cybercrime-Investigations-under-BNS.pdf

may apply if someone uses browser access to leak confidential company information, delete records, or tamper with settings. By analyzing bookmarks, browsing history, and downloads, forensic investigators can link the misconduct to the person responsible.

4.3 Role of the IEA , 1872 and BSA 2023 in Digital/Browser Forensic

The IEA, 1872, later amended by the IT Act 2000, recognized electronic records, and the BS A, 2023, modernizes this to strengthen digital evidence use; browser artifacts like history, cookies, cache, downloads, credentials, server logs, ISP/IP records, and firewall logs are admissible if authenticity, integrity, and chain of custody are proven.

4.3.1 Indian Evidence Act, 1872 for Browser Forensics

The most relevant provisions include: (i) Section 3, which defines "Evidence" and after amendment includes electronic records; (ii) Section 65A, which lays down special provisions relating to electronic records; (iii) Section 65B, which governs the admissibility of electronic records and requires a certificate under sub-section 4, crucial for browser artifacts and network logs; (iv) Section 45A, which recognizes the opinion of an Examiner of Electronic Evidence as expert testimony; (v) Section 22A, which makes oral admissions about electronic contents irrelevant unless supported by the electronic record itself; and (vi) Sections 85A and 85B, which create presumptions as to the validity of electronic agreements and secure electronic records, significant for validating digital signatures, SSL certificates, or browser security logs.

4.3.2 Bharatiya Sakshya Adhiniyam (BSA), 2023 for Browser Forensics

The parallel provisions are: (i) Section 2(1)(d) and 2(1)(e), which define "Evidence" and "Electronic Record" more clearly; (ii) Section 61, which deals with the admissibility of electronic records and parallels Section 65B; (iii) Section 63, which provides presumptions for electronic agreements similar to Section 85A; (iv) Section 64, which provides presumptions for secure electronic records and signatures similar to Section 85B; (v) Section 39, which makes electronic data such as maps, charts, and logs relevant in judicial proceedings; and (vi) Section 45, which, like Section 45A of the Evidence Act, recognizes the opinion of the Examiner of Electronic Evidence as expert testimony.

In practical application, (i) browser history, cache, and downloads are admissible as electronic records under Section 65B of the Evidence Act or Section 61 of the BSA if supported with a forensic certificate; (ii) cookies, session storage, local storage, and extensions are also treated as electronic records, their authenticity being established through forensic tools and expert certification; (iii) network logs including ISP data, firewall records, IPS alerts, and web server logs gain additional legal weight through presumptions of secure records under Section 85B of the Evidence Act or Section 64 of the BSA; (iv) expert testimony is admissible under Section 45A of the Evidence Act and Section 45 of the BSA, ensuring the credibility of forensic examiners; and (V) both Acts emphasize maintaining chain of custody to preserve integrity, with BSA 2023 offering clearer and stronger language on electronic records, thus enhancing the evidentiary strength of browser and network forensic data in cybercrime trials.

The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 marks a significant reform in the treatment of electronic and digital evidence, including browser forensic artifacts. While the Evidence Act recognized electronic records after the IT Act, 2000 amendments, its provisions,particularly Section 65B—created interpretational hurdles regarding certification, admissibility, and the scope of electronic records. Courts frequently grappled with technicalities, resulting in inconsistent rulings on whether browser logs, cookies, or ISP records could be admitted without strict compliance with the 65B certificate requirement. In contrast, the BSA, 2023 provides clearer definitions, streamlined admissibility rules, and stronger presumptions for the integrity of electronic records. By explicitly covering digital logs, maps, charts, and data sets under Section 39, and reinforcing the chain of custody requirements in Sections 61–64, the BSA creates a more robust framework for browser forensics. This ensures that Chrome artifacts such as browsing history, cache, and downloads, along with network-level evidence like ISP logs, IPS/firewall traces, and web server records, can be more effectively admitted and relied upon in cybercrime prosecutions. Thus, the BSA 2023 strengthens the evidentiary foundation of browser forensics, bridging the gap between forensic science and judicial reliability.

Forensic and Legal Significance of ISP Logs

(i) Subscriber Information Courts often rely on these logs for subscriber verification under lawful requests, such as those issued through warrants or Section 91 CrPC notices in India.

(ii) Connection Session Logs In court, such evidence is admissible when supported by proper chain of custody and certification under Section 65B of the Indian Evidence Act (or Section 63 of the Bharatiya Sakshya Adhiniyam, 2023).

4.3.3 Case Laws

This section reviews Indian cases where browser forensics—history, search logs, downloads, cache—shaped judicial assessment, showing how such evidence is examined under the IT Act 2000, IPC 1860/BNS 2023, and IEA 1872/BSA 2023, highlighting courts' reliance on browser artifacts to link online conduct with legal responsibility and strengthen cyber evidence in criminal justice.

(a) *Suhas Katti v. Tamil Nadu* (2004) : This was the first prosecution in India[41] involving obscene online content (IT Act §67) and forgery of electronic documents. Importantly**,** browser forensic evidence was pivotal—the court accepted a certified copy of relevant electronic data (like offending messages) retrieved from a Yahoo server by a private techno-legal expert under Section 65B of the IEA (as then applicable). This validated both the trial use of browser-derived digital evidence and the involvement of private forensic practitioners.

(b) *Anvar P.V. v. P.K. Basheer* (2014): The landmark judgment clarified the mandatory conditions for admitting electronic evidence, which include browser logs[42] or downloaded files. The Supreme Court held that any electronic record including browser history must be accompanied by a certificate under Section 65B(4) of the Indian Evidence Act to be admissible. This precedent reinforced the proper legal handling of browser forensic artifacts in court.

(c) Syed Ahmad Shakeel v. NIA (Delhi High Court, 8 Aug 2025) The court's narration records that the appellant's web browsing history (937 items) was analyzed, with at least one item flagged by the prosecution while assessing incriminating material[43].

(d).Riyas A @ Riyas Aboobakkar @ Abu Dujana v. Union of India (Kerala High Court, 2024) The judgment summarizes reliance on Google account data and search history, including Google/YouTube search logs and watch history, as well as other platform activity, to connect the accused with online conduct[44].

(e).Aman Siraj Mallik v. State of Gujarat (Gujarat High Court, 14 Oct 2024): The order notes investigators traced Google Chrome browser history, finding searches like "AK-47 rifles prices in India," which was treated as incriminating context in the case[45].

(f) Xxxxxx v. State of Karnataka (Karnataka High Court, 28 Jun 2023) :The court records that an iPad handed to investigators contained incriminating materials including browsing history [46]and login access relevant to the accusations; the handling/production of that device became an issue.

5. CONCLUSION

Browser forensics involves identifying, preserving, analyzing, and presenting evidence from web browsers:history, cookies, cache, logins, downloads—crucial in crimes like data theft, phishing, fraud, obscenity, and impersonation. Chrome artifacts in *C:\Users<User>\AppData\Local\Google\Chrome\User Data\Default* (History, Login Data, Cookies, Cache, Downloads, Bookmarks, Extensions) reveal user activity; tools like DB Browser, ChromeCacheView, and JSON viewers reconstruct timelines, validate actions, and detect malicious operations. Correlating browser data with DNS cache, HAR files, packet captures, and firewall/IPS logs traces attacks, recovers credentials, and supports attribution. Login Data and Web Data files expose credentials and autofill info for profiling and timeline building; bookmarks show intent; downloads trace files and attacker infrastructure when linked with AV or execution logs. Firewall, IDS/IPS, and server logs capture IPs, connections, and attack methods; email and browser traces reveal communication and intent; ISP logs link IP activity to real identities for court use. Combined browser, system, network, and application logs provide accurate event reconstruction, attack vector identification, and strong legal evidence in cybercrime investigations.

The IT Act, 2000 governs browser-based offences: Section 43 penalizes unauthorized access/data theft; Section 66 covers dishonest or repeated access; Sections 66C/66D address identity theft and online cheating via credentials, cookies, or autofill; Section 67 targets obscene content using history/downloads; Section 69 allows government interception and decryption with authorization.

Chrome artifacts like history, cache, cookies, downloads, extensions—are admissible when preserved with forensic methods, backed by ITA 2000 (Secs. 43, 66, 66C, 72). Cases include stolen banking logins (ITA 66C/66D, BNS 68), confidential file downloads (ITA 43/66, BNS 73), autofill misuse for fake IDs (IPC 419/420, ITA 66D, BNS 69), malicious extensions (ITA 66/66B, IPC 468, BNS 74), and obscene site visits (ITA 67).

[41] Suhas Katti v. Tamil Nadu, Metropolitan Magistrate, Egmore (2004) https://en.wikipedia.org/wiki/Suhas_Katti_v._Tamil_Nadu
[42] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473 : https://lawarticle.in/admissibility-of-electronic-evidence-in-indian-courts
[43] Delhi High Court, CRL.A. 262/2021 & CRL.A. 1023/2024. https://indiankanoon.org/doc/150224979 4
[44] Indian Kanoon. https://indiankanoon.org/doc/131555804
[45] Website: Indian Kanoon. https://indiankanoon.org/docfragment/88973432
[46] https://indiankanoon.org/doc/194644035

Fraud (IPC 415, BNS 318) uses browser records of transactions; forgery and falsified e-records (IPC 463, BNS 336) involve stored certificates/docs; conspiracy/abetment (IPC 120B, BNS 61) appear in encrypted chats or dark web use. IPC 1860 (Secs. 379, 420, 465, 468) and BNS 2023 (Secs. 66, 73, 74, 95) also cover unauthorized access, identity theft, tampering, and cybercrimes.

Under IEA 1872 and BSA 2023, electronic records are admissible (IEA 65B / BSA 61), oral statements alone are barred (IEA 22A / BSA 23), expert certificates validate extraction (IEA 45A / BSA 45), and presumptions cover secure records, SSL/TLS logs, and chain of custody; browser artifacts require authentication, with Section 65B IEA / BSA 63 mandating certificates for logs, while Sections 22A and 45A IEA with BSA provisions permit expert testimony on extraction methods.

Landmark cases shaped browser forensics in India: *Suhas Katti v. Tamil Nadu* (2004) admitted emails and browsing records under ITA 2000; *Anvar P.V. v. P.K. Basheer* (2014) required Section 65B IEA/BSA authentication; Delhi HC cases (CRL.A. 262/2021, 1023/2024) stressed browser artifacts for intent, timelines, and activity. These rulings confirm browser forensics as credible if authenticated and correlated, bridging technical evidence and law, with ITA governing cyber offences, BNS addressing fraud/forgery/conspiracy, and BSA ensuring admissibility for prosecution and judicial scrutiny.