THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 17

Article 4

March 2022

A CRITICAL COMPARISON OF BRAVE BROWSER AND GOOGLE CHROME FORENSIC ARTEFACTS

Stuart Berham
Cranfield University, digitalinvestigation@cranfield.ac.uk

Sarah Morris
Cranfield University, s.l.morris@cranfield.ac.uk

Recommended Citation

Berham, Stuart and Morris, Sarah (2022) "A CRITICAL COMPARISON OF BRAVE BROWSER AND GOOGLE CHROME FORENSIC ARTEFACTS," *Journal of Digital Forensics, Security and Law*: Vol. 17 , Article 4.
DOI: https://doi.org/10.15394/jdfsl.2022.1752
Available at: https://commons.erau.edu/jdfsl/vol17/iss1/4

A CRITICAL COMPARISON OF BRAVE BROWSER AND GOOGLE CHROME FORENSIC ARTEFACTS

Stuart Berham[a] and Sarah Morris[a]

[a]Centre for Electronic Warfare, Information, and Cyber, Cranfield University, Defence Academy of The United Kingdom, Shrivenham, SN6 8LA, UK,
digitalinvestigation@cranfield.ac.uk

ABSTRACT

Digital forensic practitioners are tasked with the identification, recovery, and analysis of Internet browser artefacts which may have been used in the pursuit of committing a civil or criminal offence. This research paper critically compares the most downloaded browser, Google Chrome, against an increasingly popular Chromium browser known as Brave, said to offer privacy-by-default. With increasing forensic caseloads, data complexity, and requirements for method validation to satisfy ISO 17025 accreditation, recognising the similarities and differences between the browsers, developed on the same underlying technology is essential. The paper describes a series of conducted experiments and subsequent analysis to identify artefacts created as part of normal user browsing activity. Analysis of the artefacts found that Brave and Chrome share almost identical data structures, with on-disk artefact recovery successful, even for deleted data. The outcome of this research, based upon the results, serves to enrich understanding and provide best practice for practitioners and software developers, respectively responsible for examining Chromium artefacts for use in evidence production and developing new forensic tools and techniques.

Keywords: Brave Browser, Browser Artefacts, Digital Forensics, Google Chrome

1. INTRODUCTION

Chromium based web browsers, each designed with specific features and functionality to set themselves apart from one another, presents an on-going technical challenge to those tasked with conducting digital forensic examinations. User privacy awareness continues to dominate the online world, with users now much more conscious about what data is collected and stored of their web browsing habits. This concern has seen the adoption of Brave Browser, built around the concept of privacy-by-default, grow in popularity. Privacy features include ad-blocking, anti-tracking functionality and cryptocurrency offerings. Every new browser or integrated feature can pose serious forensic implications so research must be reviewed and updated regularly.

Despite prior work conducted for the Brave Browser, there is a lack of research relating to what artefact can be recovered from the disk when using the normal browsing mode, where these artefacts are located, how they are structured, and most importantly how they compare to those found when examining Google Chrome. The requirement to understand what evidence is available becomes ever so more pertinent for ISO 17025 accredited digital forensic units, to have confidence that forensic processes are repeatable and validated, that results are accurate.

Whilst Chrome maintains the highest market share, Brave's popularity is on the increase, driven by privacy-by-default functionality. User's will typically look to transfer to browsers that look and act familiar whilst providing new functionality they require. This coupled with the fast-changing nature of browser development requires the Digital Forensics community to continuously re-examine and evaluate evidential implications. The purpose of this paper is to provide a greater understanding of the similarities and differences of analysing the latest Brave artefacts against Google Chrome which is required by both forensic practitioners, tasked with investigating civil and criminal cases, as well as forensic software developers who are tasked to automate processes for the extraction and accurate interpretation of data. The research question to be addressed is 'to critically compare normal browsing mode artefacts recovered and analysed from Brave Browser v88.1.20.110 and Google Chrome v88.0.4323.190 on Windows 10 v20H2.'

This paper critically evaluates key similarities and differences when identifying, recovering and analysing web browser artefacts. Brave Browser and Google Chrome are built upon the same open source Chromium base. However, little research exists as to the forensic implications presented when encountering Brave on a suspect's machine. Research aims to establish if existing Chrome examination tools and techniques can be extended to cover Brave and what additional challenges this presents to the practitioner. An experimentation and analysis methodology has been developed to establish what artefacts are left behind, paying particular attention to recoverability, and to determine if interpretation of their respective data structures is plausible, for evidential value. The results and findings provide the factual foundations for discussion to determine how both browsers compare and if a best practice approach is required.

To answer the research question, the methodology has been designed to implement the following objectives:

- Identify what artefacts are left behind by Brave Browser v88.1.20.110, and if they can be recovered?
- Identify what artefacts are left behind by Google Chrome Browser v88.0.4323.190, and if they can be recovered?

The essential criteria for establishing if objective 1 and 2 are met, involve the successful identification, recovery of live, and recovery of deleted artefacts from the following user activities:

- Bookmarks
- Cached images and files
- Cookies
- Browsing, Media and Search History
- File Download History

Results and findings from the first two objectives provide the criteria to assess and critically compare objectives three and four.

The remainder of this paper is structured as follows. Section 2 presents background and related work, followed by experiment and analysis methodology in section 3. Results and findings based upon the experimentation are presented in Section 4. Section 5 outlines a discussion reviewing research conducted in previous sections. Section 6 discusses future work before concluding with a summary in Section 7.

2. BACKGROUND AND RELATED WORK

This section describes related work conducted in the areas of Google Chrome and Brave Browser Internet forensics.

2.1 Internet Forensics

Internet browser forensics is a branch of Digital Forensics responsible for uncovering evidence that may assist or undermine civil and criminal cases. Research conducted in 2020 showed that out of a total population of 7.79 billion people, 4.57 billion people were Internet users. The number of global Internet users increased by 346 million in 2020 alone. (Kemp, 2020).

When investigating cyber-enabled and cyber-dependent crimes, including fraud, child sexual offences, and computer hacking, browsing activity can provide a rich source of potential evidence. (Crown Prosecution Service, 2019). Almost every action carried out by a user leaves behind artefacts that may be recovered for analysis.

One example where Internet forensics assisted in the investigation and prosecution of a person found to have committed tax fraud, by cheating the public revenue was in the case of R v Shareef. Forensic analysis of Shareef's devices found that he had created false invoices, bank statements, and VAT summaries, accessed and modified through a web browser. Shareef was sentenced in total to 11 and a half years for making fraudulent VAT repayment claims over a six-year period. (HMRC, 2016)

Google Chrome (63.54%), Safari (19.45%), Mozilla Firefox (3.64%) and Microsoft Edge (3.23%) were found to be the four leading web browsers by market share as of January 2021. (StatCounter 2021a). There is a wealth of related work into recovering forensic artifacts from the top four web browsers. Bencherchali (2019) describes some of the common artefacts stored by browsers including bookmarks, browser session, cache, history and file downloads. Many of the artefacts are stored on disk inside specific location paths within the operating system. Data is normally stored in structured files, including SQLite databases, ESE databases and JSON files, a shared characteristic between the browsers. It is not unusual for a web browser such as Google Chrome to use several file types for storing different artefacts. For example, user history is stored in a SQLite database whilst Bookmarks are stored within a JSON file. Through structural analysis of these files, the user activity can be reconstructed.

When conducting a forensic examination of a web browser, it is not appropriate to only analyse one file, as evidence is often split over many separate but linked files. (Jadhav & Meshram, 2018). This fragmentation of evidence, coupled with the fast pace of browser innovation often causes the identification and analysis of artefacts to become outdated.

In addition to the four leading web browsers, there has been a rapid increase in the release of alternative browsers, with user privacy at their core. Since the 2013 unauthorised leaks of classified data by NSA contractor Edward Snowden, public awareness of how online data is collected and used by third parties has received increased scrutiny. (Daniel, 2018).

2.2 Google Chrome Overview

Google Chrome is a cross-platform web browser released in 2008. As of January 2021, it accounts for the largest browser market share of 63.54% (StatCounter 2021a). As of writing this paper, the latest version is 88. Due to its popularity among users, it also attracts attention from the digital forensic community to better understand evidential opportunities and challenges posed when encountering Chrome in an investigation. The identification of artefacts and their respective locations are well documented in prior research.

A practitioner conducting an examination will encounter an extensive range of artefacts, including bookmarks, cache, cookies, current tabs, history, sync transfers, and last session data. (Malviya, 2020). The research provides path listings of where each artefact is stored on the Windows operating system and tools for performing browser forensics. Shafqat (2016) describes how the history file alone was sufficient to reconstruct a timeline of the user's activity. Enough to establish intention.

2.3 Brave Browser Overview

User privacy awareness is a key contributing factor for the development of the free and open-source Brave Browser. Brave was founded by Brendan Eich who was a co-founder of the Mozilla project, and Brian Bondy who previously worked on Mozilla's Firefox browser. Brave's design philosophy is based on providing privacy-by-default ad-blocking, script blocking and anti-website tracker capabilities, whilst rewarding users through a crypto opt-in reward scheme. (Wilson, 2018).

Brave is developed upon the open-source Chromium browser project which promotes faster, safer browsing. As the project is open source, Brave is able to make use of the code for their own product, adding additional features on top. This is also the same base that Google Chrome bases its browser on. (Keizer, 2020)

Statistics compared from 2020 to 2021 show the monthly active users increased from 11.6 to 25.4 million. (Brave Blog, 2021). While this number is still only a fraction of the 63.54% browser market share that Google Chrome commands, it highlights a continuous upwards growth in demand, potentially impacting digital investigations.

Reed et al. (2017) describes how serious organised crime, alongside individual users are benefitting from privacy driven browsers such as Tor and Epic Privacy browsers to conduct money laundering, distribution of drugs and to trade in indecent images of children. This view is further supported by Mahlous & Mahlous (2020), who conducted a study of privacy preservation in the Brave browser to suggest that criminals have gained more awareness of private browsing functionality, using them to cover their tracks when conducting criminality.

2.4 Overview of Brave Browser Forensics Research

Brave browser forensics is still in its early infancy with little related work identified. Benson (2016) noted the structure of recovered artefacts was very similar to Chrome which is not surprising considering the shared Chromium foundation. A number of Local Storage, IndexedDB and database folders were present however there was also a number of files missing, notably the History SQLite database. Differences between Brave and Chrome included additional partition folders which contained their own cookies, cache and local storage.

As previously outlined, Brave adopting the Chromium base often provides less features than found in Chrome. In Brave version 0.8, the Cookie values were found to not be encrypted but were however in Chrome. (Benson, 2016). This can possibly be explained by the maturity of Chrome versus newer browsers which encounter slower adoption of features, and differences in design implementation, notably seen around privacy functionality.

A recent study published by Mahlous & Mahlous (2020) focused on privacy preservation in Brave browser on Windows 10. The aim of the study was to examine which artefacts and where on the system they could be recovered when using the private browsing mode. The study identified that artefacts only existed when conducting live RAM analysis and dead box forensics from the disk produced no evidence. The RAM extracted artefact results were similar to those from Chrome, Epic, Browzer and Commodo Dragon, sharing almost identical locations. To compare artefacts recovered from private mode browsing, an identical experiment was conducted using the normal browsing mode. The results of the normal browsing mode provided a number of on-disk files and directory locations for browsing data but did not elaborate further.

Magnet Forensics identified a limitation that Chromium based browsers with similar backend design can cause an issue for recovery of carved records as it can be difficult to determine from which browser the data came from. (Magnet, 2017). This is especially true if both browsers are installed on the same suspect system. Even if only one browser is found installed, there is an increased risk that artefacts may be misinterpreted by both forensic software tools and practitioners if not identified and examined correctly.

3. METHODOLOGY

This section describes the experiment and analysis design considerations for the resources required to conduct the study.

3.1 Experiment Strategy

To conduct experiments to answer the research question and objectives, as outlined in section 2, hardware and software are required. The primary tools include a laptop capable of running multiple virtual machines, Windows 10 operating system and virtualisation software.

Research was conducted using a forensically wiped Dell XPS laptop with a clean copy of the Windows 10 v20H2 operating system and the latest security patches installed. Windows 10 was installed from the University's Azure Student Portal. Window 10 was chosen as the base OS as it commands 76.26% of the desktop operating system worldwide market share, as of January 2021. This is compared to 16.91% for Apple OS X and 1.91% for Linux distributions. (StatCounter, 2021b) Both web browsers are also fully supported on Windows 10.

VMWare Workstation Pro 15 supports the running of multiple virtual machines in parallel, isolating each from one another and the underlying physical host system. Windows 10 was installed onto a clean Virtual Machine (VM) with a virtual 20GB hard drive and 8GB of RAM. One user account named 'research_machine' was created. After Windows was installed, a registry snapshot was captured and VM cloned; the original machine was kept to provide a baseline for experiments, identified by reference VM_Base_Image. Google Chrome v88.0.4323.190 was next installed onto a copy of the cloned machine to provide the second experimental VM, referenced as VM_Chrome, followed by a third clone containing the Brave Browser installation (v88.1.20.110), with reference VM_Brave. The hard drive was kept at 20GB to satisfy the OS installation requirements, whilst decreasing the time required to run data carving and keyword search term analysis.

The use of multiple cloned virtual machines is important when critically comparing Brave against Chrome, as research from Magnet Forensics suggests the use of more than one Chromium browser on a target system can cause confusion when trying to recover deleted artefacts. As the same dataset is used for both browsers, this will limit misinterpretation during analysis. (Magnet Forensics, 2017)

Figure 1 provides an overview of the experiment methodology. Virtual machine snapshots at key interactions with the operating system and web browser, creates a differencing virtual disk, where all changes are written to that differencing disk from that point in time. (Bose, 2018). Virtualised snapshots provide a forensically sound method for limiting variables and user activity at each experiment stage, integral to identifying artefact changes. Highlighting if an operating system or user action caused a change to an artefact ensures accurate findings when critically comparing each browser. Refer to Appendix A – Table A1 for a descriptive breakdown of each VM snapshot. During the experiment and analysis phases of the research, contemporaneous notes using Microsoft OneNote recorded the date and time that each action was taken. This includes all user interactions with each web browser and use of analytical tools outlined in this section.

Experiments are designed to mimic typical user interaction with a browser using the normal browsing mode to establish the artifacts left behind. User activity is populated through the use of typed searches, navigation of website URLs and file downloads. Search terms include unusual strings to facilitate keyword searching during analysis, limiting false positives. To facilitate file downloads, two images were randomly selected and downloaded from the landing pages of amazon.com and fetch.co.uk. A third image was selected from Google Images using the search term 'Flags' and saved to disk. To create web streaming data, the search term 'cats' was searched on youtube.com, with the video entitled 'CATS will make you LAUGH YOUR HEAD OFF - Funny CAT compilation' watched for 10 seconds. During selected deletion of data, the file download history entry for DogLeft.png, downloaded from fetch.co.uk was deleted from within each browser.

The process for populating then deleting selective user activity is provided in Table 1.

3.2 User Browsing Activity

Interaction with the browser occurred over the space of 1 hour, primarily to limit date and time stamps, useful when conducting low level binary analysis, and searching across the virtual disk.

3.3 Analysis Strategy and Tools

Third party forensic software tools are required to fulfil the needs of the analysis strategy, firstly to locate each artefact on-disk, followed by the recovery, interpretation and attribution. Tools in this section are installed on the physical host machine to avoid contaminating the experiment virtual machine environments.

Analysis of each experiment for each artefact, from each browser is conducted independently to allow the findings to be assessed in Section 4. Figure 2 provides an overview of how each artefact is analysed.

Each VM snapshot taken during experimentation is stored as separate VMDK container files.

AccessData FTK Imager V4.1.1.1 (AccessData, 2017) was chosen as it supports the mounting of such containers. FTK Imager also provides a directory tree viewer to navigate the disk image, forensically hash items of interest, and export live files for further analysis in secondary tools. The most suitable software tools for artefact analysis depend on the file format. Selected tools required for this research are:

- X-Ways WinHex v20.1
    - For low level binary analysis
    - For keyword searching

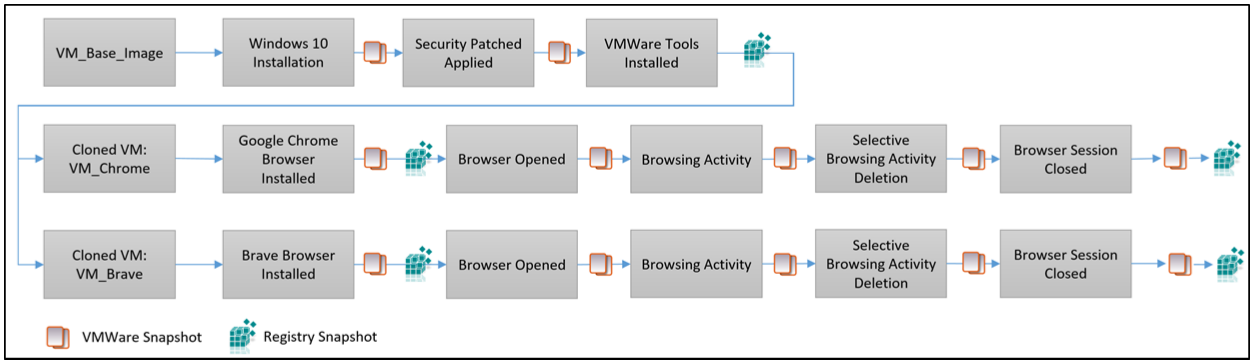


Figure 1. Experiment Process Model

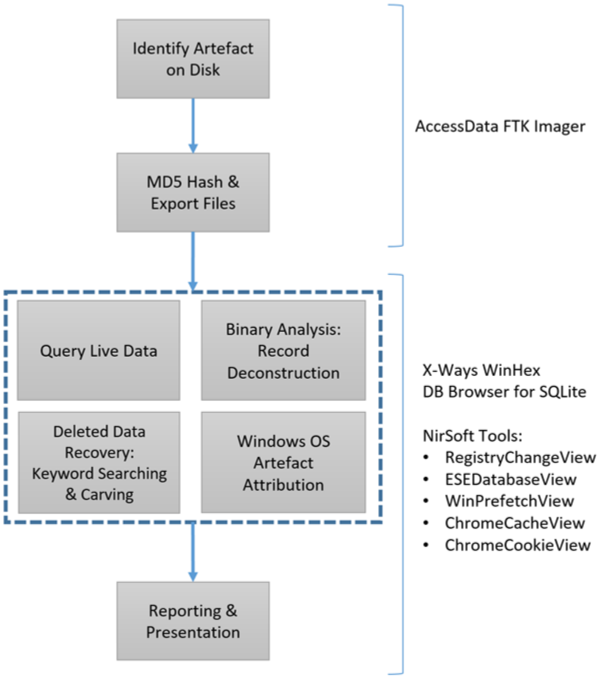


Figure 2. Analysis Process Model

  - For data carving - recovery of deleted records
  - For reconstruction of artefacts

- DB Browser for SQLite v3.12.1 for Windows
  - For running SQL queries which provides an indication of deleted records through missing row ID.

- Nirsoft tools:
  - RegistryChangeView v1.27
  - ESEDatabaseView v1.65
  - WinPrefetchView v1.36
  - ChromeCacheView v2.25
  - ChromeCookieView v1.85

WinHex's core functionality supports simultaneous searching across multiple character sets and carving at binary level, across a range of file formats including those frequently encountered from Internet browsing activity. Files typically requiring examination from a browser include SQLite binary databases, Extensible Storage Engine (ESE) databases and JSON files, which are fully supported by this tool.

For artefacts such as History, an SQL viewer is required to read the database format. DB Browser supports executing search queries, and exporting of returned results. Areas of interest are database and table schemas which, when interpreted may indicate what type of data is stored, how that data might be split across multiple tables, and most importantly, the data structures of individual records within those tables.

Nirsoft tools developed by Nir Sofer provide analysis capability for specific browser features including Cache and Cookies. RegistryChangeView is selected to capture and review changes to the Windows Registry, prior

Table 1. Experimental Activity

Tab	URLs Visited	File Downloads	Searches
1	www.bbc.co.uk - Click on BBC News	www.amazon.com **Brave**, JPG - filename: Mday21_Desktop_Cat_-Card_2_379x304._SY304_CB660441972_.jpg. **Chrome**, JPG - filename: XCM_CUTTLE_1311643-_1599235_UK_3697498_379x304_en_GB._SY304-_CB658598983_.jpg	
	www.just-eat.co.uk	www.fetch.co.uk/ - PNG filename: DogLeft.png	
	www.game.co.uk	www.images.google.com/ - JPG filename: gn0547-flags-of-the-world.jpg	
2			www.youtube.com - Search 'cats' and watch 10 seconds of video titled: 'CATS will make you LAUGH YOUR HEAD OFF - Funny CAT compilation'
			www.wikipedia.org - Search 'education' and click the first link
			www.bbc.co.uk/weather - Search 'London'
3			www.google.co.uk - Search: 'santander', 'A1S2D3F4G5' and 'Z9X8C7V6B5'
4	www.monzo.com - **add bookmark**		Address bar search (Google) - 'hexagon', 'pentagon' and 'rhombus'
	www.hsbc.com –**add bookmark**		
Browsing Data Deletion		Close tab 2 followed by closing tab 3	
		Delete Bookmark: www.monzo.com	
		Delete Browsing and Search History o just-eat.co.uk o Education - Wikipedia search o Search term 'A1S2D3F4G5' o Search term 'pentagon' o 'cats - YouTube'	
		Delete fetch downloaded image from list	

to and after browser installation. ChromeCookieView offers decryption of the encrypted cookie value, added into Chromium since v80 onwards. All results produced by third party tools are dual verified using manual techniques in WinHex where appropriate.

4. RESULTS & FINDINGS

This section outlines the experiments conducted for each browsing artefact and their respective results. Results for each browser are grouped under each artefact for comparison. Using the base image to produce a clone for Brave, and a second for Google Chrome, several experiments were conducted to identify how artefacts compare between each browser. During the user browsing activity as outlined in section 3.2, a series of typical user actions were performed to cause artefact interaction. Once experiments were completed, the analysis strategy was implemented, with each artefact analysed independently.

4.1 Windows Registry

The first experiment required the use of Nirsoft RegistryChangesView v1.27 to review system changes of the base VM registry prior to browser installation and subsequent snapshot taken directly after browser installation. RegistryChangeView generates an Excel spreadsheet, detailing new files and folders added as registry keys and values. This exercise was completed separately for both browsers, to avoid misinterpretation of results. Analysis of the registry is used to identify the software installation process, and initial setup behaviours which provided the version identifier, and paths to the installation directories.

A keyword search of ‘Google’ on the Registry Key column produced 358 hits in the Software hive. A further filter applied to column ’Value Data’ for ’Google’ narrowed down hits to 103 entries. The registry stores keys and values identifying the Chrome version installed: 88.0.4324.190 and installation path of the executable file, found at ‘`C:\Program Files\Google\Chrome\Application\chrome.exe`’.

For Brave, the same ’Google’ keyword search on the same Registry Key column produced slightly more hits at 367. The second applied filter produced a smaller return of 84 hits. Both version and publisher identifiers, alongside installation paths, observed with Chrome, are provided. Brave version identified as 88.1.20.110 with program data found at ‘`C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe`’.

4.2 Browser Application Structure

Examination of the registry provided the default installation location of the application system files, for Brave found at `C:\Program Files\BraveSoftware\Brave-Browser\Application\` and for Chrome found at `C:\Program Files\Google\Chrome\Application\`.

The VM user account ’research_machine’ was found to store locally generated artefacts at `C:\Users\[username]\AppData\Local\BraveSoftware\Brave-Browser\User Data\` for Brave and `C:\Users\[username]\AppData\Local\Google\Chrome\User Data\` for Chrome. A sub-directory entitled ‘Default’ contains the majority of artefacts of interest including `Bookmarks`, `Cache`, `Cookies`, `History` and `Session` data. Appendix A - Figure A1 provides a side by side comparison of the similar looking structure.

Comparison proves that both browsers implement a similar directory and file structure, with identical naming conventions. Further analysis of the VM snapshots highlighted that additional directories and artefact files are created upon opening the browser and starting the browsing activity. Observation saw bookmarks, and last sessions and tabs, only created on disk for that particular user when that feature was initiated.

4.3 Browsing History

The History SQLite database is responsible for the storage of typed search terms and inputted web URLs in the browser address bar, and search engines. The database does not contain a file extension but upon binary examination, a SQLite header is present. SQLite is implemented using B-Trees which provides a self-balancing mechanism that maintains data storage, searching, new insertions and deletions. Separate B-Trees are used for each table and index in the SQLite database.

To meet objectives one and two of this research, the artefact must be identified, and data recovered. The location of the History browsing database for Brave, and Chrome is respectively found at ‘`C:\Users\[username]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\History`’ and ‘`C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\History`’. An associated file named `History.journal` is also present but was found empty during binary analysis.

Opening `History` in DB Browser for SQLite identified 12 tables and 11 indexes. Table structure including column names and data types were identical for both browsers. The test data was compared to the active records by producing an SQL query that linked tables: `urls` and `visits`. Live records show 47 entries in Chrome and 60 entries in Brave. To filter for unique records related to the transition value, the SQL query was updated as shown in Appendix A (2021) - Figure A2. This resulted in 19 records in Chrome and 22 in Brave. The difference being Chrome lacked some entries when entered website URLs were redirected to HTTPS. All expected test data that was not deleted during the experimentation process is present. Both browsers reported 7 deleted rows in table: `urls`.

Manual validation of the findings was conducted using binary SQLite analysis of the History database. Deconstruction of the SQLite file header showed that Write Ahead Logs (WAL) was not set, auto-vacuum off and no free pages detected. The header, leaf table and record payload were successfully deconstructed. This process involved interpreting multi-VARINT values to identify each record's length and corresponding values. An example is highlighted in Appendix A (2021) – Figure A3 and Table A2. The records displayed by DB Browser for SQLite matched the raw binary structure.

Text and hexadecimal keyword searching within the History database using WinHex failed to identify any deleted browsing activity. Related work suggested that partial fragments from deleted records may be present; however it was observed that where deleted records may be expected that those sections were zeroed out. A manual review of the binary also failed to identify deleted data. Review of VM snapshot 6 showed the same area of binary zeroed out. This infers that closing the browser session did not impact when data was deleted but rather was caused by a time based, application or operating system feature driven process.

Hex & ASCII keyword terms for deleted test data:

- 41315332443346344735 (A1S2D3F4G5)
- 70656e7461676f6e (Pentagon)
- 6a7573742d6561742e636f2e756b (just-eat.co.uk)
- 456475636174696f6e (Education)
- 63617473202d20596f7554756265 (cats - YouTube)

Keyword searching was extended to search the full OS partition, for both browsers. Only the two typed search terms ''`A1S2D3F4G5`' and '`Pentagon`' for Chrome using the Google search engine were partially identifiable, found in Chrome artefacts: Session Storage log named `000003.log`, Local Storage LevelDB log named `000004.log` and Windows Storage DataSharing ESE database named `DSSres00001.jrs`.

On inspection of the artefacts, most hits only referenced the searched term; however, the file named DSSres00001.jrs contained the full Google search URL that pointed to the web page when accessed. The hits could not be forensically attributed back to the History database. The same keyword searching for Brave produced hits in free space and pagefile.sys. All deleted records from the url table were successfully located, deconstructed, and carved, providing of interest, the original row ID, url and timestamps. As all deleted entries were present, a SQL file header search was conducted but failed to identify the full database for carving.

4.4 History Provider Cache

An additional source for history data is the History Provider Cache, structured as Google Protocol Buffers. The file contains only visits and predates information found in the main History database. Deleted history search terms in both ASCII and their hexadecimal equivalent where not found.

4.5 File Download History

Metadata relating to the files downloaded through the browser are stored in the same History SQLite database as browsing history. The analysis process outlined in Section 4.3 was repeated for file downloads, first to confirm the presence of data, identify if any records were deleted, and attempt to recover using browser and wider OS artefacts.

As discussed in Section 3.2, three images were downloaded during the data population process before the file download history entry for file named DogLeft.png was deleted. An experiment was constructed using SQL queries to join tables: downloads and downloads_url_chains from the History database. Two records with row ID 1 and 3 were found to be present. Row ID 1 corresponded to the image downloaded from Amazon.co.uk, and row ID 3 corresponded to the image of flags downloaded from Google Images. Data present in the row included the GUID, current file path, start time of download, received bytes, total bytes, end time of download, accessed status, last accessed time, URL site referrer and last modified timestamp. Row 2 was not present and presumed deleted, in line with observed browsing table behaviour.

Binary SQLite analysis verified that DB Browser had accuracy interpreted the database. This was followed by inspection of the column named current_path which indicated that downloads by default are saved to the user's Download folder. Review of the Downloads folder found an image named 'DogLeft.png'. The file's timestamps showed that it was downloaded within one minute of the two other graphics present in the folder, matching the experiment user activity. A keyword search in ASCII and hexadecimal failed to return any hits from the History database. Wider OS artefacts were reviewed to aid in the recovery of missing row ID 2, assumed to be the metadata relating to DogLeft.png.

4.5.1 Chrome

A full disk keyword search for the text and hex term 'DogLeft' produced multiple hits in free space, pagefile.sys and ntuser.dat. Unfortunately, the hits related to the actual image file and not to the corresponding database record. Hits in the Chrome log named 00003.log, part of shared_proto_db found the GUID, URL, referrer URL, downloaded last modified timestamp, mime type and download path. This binary data was found to be positioned between the binary of the other two downloaded files. Additional hexadecimal searching of converted timestamps failed to provide remaining metadata expected in a file download record row.

The final 3 hits successfully recovered the complete database record from SRUDB.dat, an ESE database, located at C:\Windows\System32\sru. Windows System Resource Usage Monitor (SRUM) contains information about machine activity, by monitoring desktop application programs, services, and network connections. Like the data found in shared_proto_db, the deleted record was positioned between the two existing live records. Appendix A (2021) – Figure A5 shows the recovered database record. This experiment highlights that analysis of browser only artefacts is not always sufficient as in this example, the missing database row was identified from analysis of a wider OS artefact.

4.5.2 Brave

Conducting the same examination for Brave, a similar number of hits containing metadata relating to the DogLeft.png file were found in free space. The database record could not be recovered however, similar data to that extracted from the Chrome log in the shared_proto_db directory, was discovered in a log also named 00003.log but was instead located in the C:\Users\[username]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default directory, providing GUID and URL referrer metadata. The SRUDB.dat ESE database in the Brave VM did not contain the missing row ID entry.

4.6 Windows OS Artefacts

To complement browser artefacts, a number of Windows OS artefacts were investigated, guided by search term hits. OS artefacts recovered included Alternative Data Streams (ADS) attached to the downloaded graphic files, Windows Desktop Search and Windows Prefetch.

ADS provided the host URL, which enhanced the examination as this piece of metadata is not stored in the History database, and useful for additional searching. The ZoneID with value 3 showed that the graphic files were downloaded from the Internet using a web browser.

The NirSoft ESEDatabaseView tool facilitated the parsing of Windows Desktop Search (WDS), an ESE database, found at C:\ProgramData\Microsoft\Search\Data\Applications\Windows\, providing a wealth of graphic metadata including modified, accessed and created timestamps, file size, colour profiles and paths. This artefact is useful for demonstrating user activity conducted around the same time.

During experimentation, each graphic was opened after download through the browser. Prefetch, a Windows artefact, found at C:is responsible for the loading of resources before they are required to decrease the time waiting. Using a second NirSoft tool named WinPrefetechView, it was shown that the three images including 'DogLeft.png', downloaded from the fetch.co.uk website were accessed within 1 minute of one another.

The linked association between browser artefacts and Windows OS artefacts can be seen in Figure 3. A corresponding table explaining relationships between each node can be found in Figure 4.

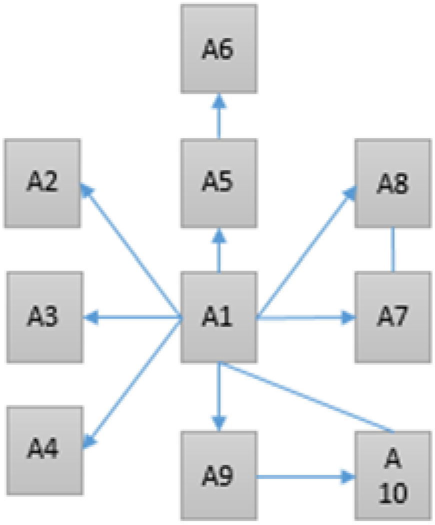


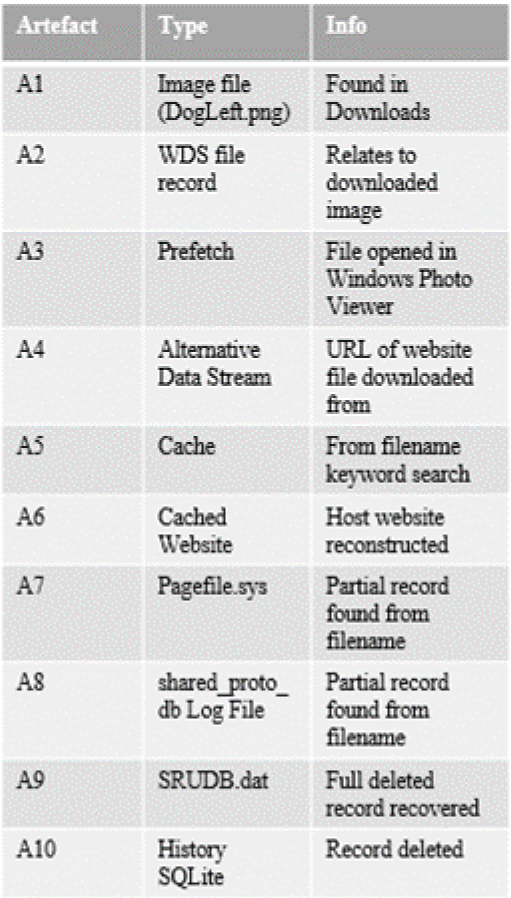
Figure 3. Artefact Association Diagram

4.7 Cache

Browser Cache is a temporary storage method for static assets such as webpages and images that do not typically change, used to reduce bandwidth and load commonly visited sites faster. Forensic analysis of Cache provided a great wealth of recoverable live and deleted data. Both browsers were found to have implemented the same structure, with data blocks starting with the string 'Data' and data files starting with the letter 'F', each followed by an incremental hex counter.

Chrome stores Cache at C:\Users\[username] \AppData\Local\Google\Chrome\User Data\Default\Cache, whilst Brave Cache at: C:\Users\[username]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache.

NirSoft ChromeCacheView v2.25, parsed and recovered all live and deleted records,



Artefact	Type	Info
A1	Image file (DogLeft.png)	Found in Downloads
A2	WDS file record	Relates to downloaded image
A3	Prefetch	File opened in Windows Photo Viewer
A4	Alternative Data Stream	URL of website file downloaded from
A5	Cache	From filename keyword search
A6	Cached Website	Host website reconstructed
A7	Pagefile.sys	Partial record found from filename
A8	shared_proto_db Log File	Partial record found from filename
A9	SRUDB.dat	Full deleted record recovered
A10	History SQLite	Record deleted

Figure 4. Artefact Diagram Relationships

displaying additional fields such as `server IP`, a value not populated in the `History` database. The reported metadata matches other collaborating artefacts including the recovered record from `SRUDB`.dat. Manual verification of the tool was conducted with WinHex and found no data inaccuracies. ChromeCacheView also encountered no issues in parsing Brave's Cache.

Extraction and reconstruction of the data files lets the practitioner review the cached copy of the webpage. Appendix A – Figure A5 provides an example of the deleted just-eat.co.uk browsing record.

4.8 Bookmarks

Brave and Chrome were found to store user bookmarks in a JSON file. Chrome bookmarks are stored at `C:\Users\[username] \AppData\Local\Google\Chrome\User Data\Default\Bookmarks` whilst Brave stores at `C:\Users\[username]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Bookmarks`.

Two bookmarks were added during the experiments, related to banking websites hsbc.com and monzo.com. The `monzo.com` bookmark was deleted. Analysis of the JSON file in Sublime Text 3 provided only the live `hsbc.com` bookmark, containing its `name, URL, bookmark folder, date added and timestamps`, including a synced timestamp.

Keyword searching to aid in identifying the deleted bookmark using the structure of the existing JSON bookmark failed to produce hits on the disk image for either browser. Closer inspection of Brave, identified two temporary and marked as deleted by WinHex, bookmark files. One empty (Bookmarks∼FR1122b8.TMP) but the second named Bookmarks RF15dd79.TMP containing the deleted Monzo bookmark.

4.9 Cookies

Cookies are files created by websites visited as part of normal user browsing. Both browsers store cookies in an identically structured SQLite database, located for Chrome at `C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Cookies` and for Brave at `C:\Users\[username]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cookies`. Review of the database using DB Browser identified 182 cookies present in table: cookies for Chrome and 87 cookies for Brave. An SQL query filtering for records related to 'bbc.co.uk' found 10 hits returned for Chrome but only

5 for Brave. Appendix A – Figure A6 shows the SQL query.

Cookie values are encrypted since Chromium version 80 onwards. These are stored in the table: cookies, column: ‘`encrypted_value`’. Nirsoft ChromeCookieView v1.85 is the tool of choice to decrypt cookie values. The decryption process requires the user login password, Local State file and Protect Folder found at `C:\Users\[username]\AppData\Roaming\Microsoft\Protect` from each browser. ChromeCookieView was successful in decryption for both browsers. WinHex binary deconstruction of a sample bbc.co.uk record was conducted to confirm tool accuracy.

4.10 Media History

One Youtube video was briefly played as part of the experiment. This activity was discovered in the Media History SQLite database, located for at `C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default\Media History` for Chrome and `C:\Users\[username]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Media History` for Brave. The video was played for 15 seconds during Chrome experimentation and for 19 seconds in Brave. Both values were successfully recovered. Appendix A (2021) – Figure A7 provides the SQL query used to extract the record.

The database interestingly records if the media has `audio` and `video`, `title` and `artist` of the media item, and a `URL` that links to the static video image, in the case of the YouTube video. This is of forensic importance as it assists the practitioner to demonstrate that the user had an awareness of the video content before clicking through to start said item, followed by the duration of the video played.

4.11 Brave Attention Tokens (BAT)

Analysis of the core browsing artefacts showed little to no difference between Brave and Chrome. Upon further inspection of Brave, a directory named `ads_service` was found in the `..\User Sata\Default` folder. There contained a SQLite database named database.sqlite and four JSON files named ‘`ad_conversions.json`’, ‘`client.json`’, ‘`confirmations.json`’, and ‘`notifications.json`’.

According to Brave (2021), their Basic Attention Token (BAT) is a way of rewarding users who spend time visiting content creators and advertisers, signed up to the scheme. The browser automatically starts tallying up the time spent on each site visited. Brave adds that this tally is only stored on the device’s local disk. Analysis showed that the artefact was turned on by default, with the `ad_service` directory appearing during browsing activity between VM snapshot 2 and 3.

During the course of populating user browsing activity in the browser, 3 adverts are found in the `ad_events` SQLite table. Two of type ‘`ad_notifications`’ and one ‘`new_tab_page_ad`’ were recorded. Linking `database.sqlite` data against `confirmations.json`, it was possible to determine that the current payments balance for month: 2021-03 was 0.0, however this value only updates by one decimal place. The true balance was 0.07, with three ads being recorded as viewed in the JSON `transaction_history` tag. Appendix A (2021)– Figure A8 shows the transaction balance.

Forensically, this provides a new artefact to identify time spent interacting with a browser, and possible cryptocurrency links. The evidential value cannot be overlooked so was added to research scope.

5. DISCUSSION

The first two objectives of the research question are to establish if Brave Browser and Google Chrome artefacts could be successfully identified and recovered when a user operates in normal browsing mode on a Windows 10 machine. Experiments were devised to supply sufficient user browsing data to populate core artefacts; Cache, Cookies, Browsing, Media and Search History, and File Download History.

It was observed that Brave Browser and Google Chrome stores user generated artefacts from normal browsing mode on disk, that remains persistent, even after closure of the browser session and shutdown of Windows 10. Implementing a combination of third party parser and visualisation tools, with manual binary level verification ensured accuracy of interpreted results.

The history file provides sufficient information to reconstruct a user's browsing activity, from typed URLs and search engine keywords to downloaded files. This can be complemented with cached data which provides locally saved copies of websites that the user has visited. For the forensic practitioner, these two artefacts combined show that the device had conducted the activity in question.

Browser artefacts, located in the user's local AppData folder structure, have been recovered from the experiments including typed URLs, keyword searches and graphics. URLs and keywords were primarily found in the History SQLite database, alongside file downloads, whilst graphics were abundant in Cache. Cache plays an important role when identifying and recovering deleted data. Often in forensic investigation, the examination strategy will focus on an initial starting point, which may surface from a search term hit or time frame of interest, to determine what artefacts should be examined first. Analysis from both browsers showed that Cache provides the opportunity to reconstruct websites and review graphics. However, they are stored in data blocks without file extensions so the data files must first be interpreted to identify pointers.

Related work indicated that deleted data may be stored within browser artefact data structures however analysis indicated that this was not the case for SQLite databases using the legacy write format, and for JSON files. When records are deleted, the SQLite B-Tree structure is modified so records are moved from node to node. The forensic implication is once data is marked for deletion, the tree must be rebalanced, allowing for elements to be moved among nodes, or whole nodes to be rearranged within the database. Nodes contain unallocated space which may contain deleted or modified data however, analysis failed to identify or recover any of the deleted search terms from the History database. Binary located between table records, identified as potentially once containing the now deleted data, were zeroed out.

Even with the lack of recoverable data from the browser artefacts internal structures, wider operating system artefacts were successful in either recovering the full deleted record, attributed back to the browser database table, or as a minimum provided partial references. The forensic implication to this approach is that the user activity test data was known beforehand so search terms could be crafted however in real life investigation, these would not necessarily be known and could be difficult to identify without prior intelligence.

As is common practice in forensic investigation, artefacts should be collaborated to build up a timeline of user and system activity, showing how one action caused a change elsewhere. Using a downloaded graphics file as the starting point (DogLeft.png), it was possible to visually show how a combination of browser and OS artefacts were related, strengthening evidential value.

The artefacts selected to compare Brave Browser critically and Google Chrome were shown to be identical in location, internal data structure and operation. Each artifact's internal configuration also appears identical, observed through deleted database records being zeroed out when the binary was examined.

Related work by Benson (2016) suggested that Brave's development was behind that of Chrome so artefacts such as Cookies might appear different however this was not found to be the case. Findings confirm that both browsers are now running Chromium version 80+. ChromeCacheView and ChromeCookieView accurately parsed and interpreted Brave's artefacts. Browser implementation of Chromium version 80 onwards provides a consistent examination approach, further supporting forensic practitioners and software developers.

The key differences did not come from the core artefacts but the additional of Brave specific features. Whilst out of initial research scope, the incorporation of cryptocurrency wallets and privacy advert system produced artefacts not observed in Chrome.

The research provides forensic practitioners and software developers with the confidence that investigations involving the latest versions of Brave Browser and Google Chrome at this time of writing, can be examined using the same tools and techniques, producing the same findings for the core artefacts. The ISO 17025 standard focuses on the competencies required for testing and calibration laboratories. This research is not intended to provide a method for use in an investigation, but rather to identify areas of interest in the Brave Browser and determine how they relate to those in Google Chrome. By following the research methodology, those technical staff responsible for implementation of ISO 17025 accreditation can replicate and reproduce findings to ensure a consistent approach when investigating browser artefacts in a forensically sound manner. This research and associated results can also be used by laboratory staff to aid in creating tests or validating software designed to extract data relating to Brave Browser activity.

5.1 Limitations

Upon reflection of the chosen methodology, user browsing test activity could be refined. Each artifact could instead be populated and individually snapshotted rather than populating data followed by snapshots at key moments. This would simplify analysis when multiple search hits are found in multiple disk locations, ensuring that the expected artefact was indeed the one that generated the hits.

To avoid misinterpretation of results and findings, each browser was installed in a separate VM. In a real world investigation, it would not be uncommon to encounter multiple browsers on the same machine. This would add complexity to analysis but nonetheless represent real world findings.

Experimentation methodology specified two periods of five-minute time intervals where no user interaction with the browser occurred. The first after user browsing, and second, after deletion of browsing activity. This may have had an impact on why some deleted artefacts were found on disk, in locations including free space and pagefile.sys, whilst others were not recoverable.

The original methodology contained the artefact 'last sessions and tabs' however, difficulties were encountered in the deconstruction of the Session Saver (SNSS) file format. Whilst keyword terms were identified and content appeared consistent for both browsers, the binary structure could not be parsed to an adequate standard, to be able to provide factual results and findings. For this reason, it was removed from artefact scope.

6. FUTURE WORK

Experiments were conducted using virtual machines rather than physical hardware to provide a more realistic environment when researching user activity behaviour. There is a lack of research that looks at virtualization's accuracy compared to physical hardware when conducting digital forensic research.

The research tested each browser in separation to simplify the process of identifying and recovering artefacts. Further research could investigate what, if any, forensic implications are present using multiple Chromium browsers on the same system.

Another area of forensic interest would be to compare Brave to other Chromium based browsers, identifying key differences which may pose forensic challenges.

Finally, further work is recommended to identify forensic opportunities of how Brave specific artefacts are linked and structured, paying particular attention to the Brave Attention Token (BAT). BAT is a crypto asset system that pays publishers for their content and rewards users for their attention, by viewing targeted adverts. Brave's incorporated Binance widget makes it the only browser currently on the market to integrate functionality for buying and trading cryptocurrency. Examination showed the presence of an advert artefact, recording the adverts presented to the user, frequency and balance of the user's crypto wallet.

7. CONCLUSION

In conclusion, the literature review discovered a lack of Brave Browser research, with related work identifying differences in recoverable artefacts and their data structures. This paper has shown that Brave Browser artefacts are located and structured in an identical format to those recovered from Google Chrome. The latest version of Brave did not reflect findings from related work, with artefact structures updated to the latest Chromium version, in keeping with Chrome. An experiment and analysis methodology was conducted using best practice guidelines, ensuring that the results were accurate and repeatable.

The majority of user activity was discovered in the History SQLite database, storing typed URLs, search terms, and file download history. Whilst deleted records were not recoverable from the History database, Windows 10 system artefacts were shown to store either full records attributed back to the database, or partial fragments, still of evidential value. It was further discovered that the browsers adopt many storage file formats including SQLite, ESE and JSON files.

It was observed that more than one browser artefact stores similar structured data which can be harnessed during examination. Where deleted browsing and search records could not be recovered from History, Cache provided the full history with website and graphic fragments, enough evidence to determine the order in which the experimental user activity was conducted in.

Similarities between both browsers proved unexpected, with identical location, file format, and binary deconstruction of data structures. Nirsoft tools developed for Chrome, successfully parsed and accuracy interpreted Brave artefacts, supporting this finding.

Key differences came in what data was populated in those files, namely Brave storing considerably less Cookies, likely explained by cross-site cookie blocking enabled by default. Brave offers unparalleled privacy and security which was observed by a significantly lower number of cookies stored, 87 versus. 182 stored by Chrome. Whilst this has a negative evidential impact, the wealth of other data stored in remaining artefacts such as user timeline activity and reconstruction of events, mitigates much of this loss. It was also highlighted that Brave has additional artefacts including Brave Attention Tokens (BAT) which should be investigated further, possibly providing further evidential value.

In summary, research findings assure that Chromium based Brave Brower and Google Chrome can be forensically examined using the same tools and techniques for artefacts shared between both, in normal browsing mode including Cache, Cookies, Browsing, Media and Search History, and File Download History.

REFERENCES

[1] Bencherchali, N. (2019). Web Browsers Forensics. Retrieved on 13 February 2021 from https://nasbench.medium.com/web-browsers-forensics-7e99940c579a

[2] Benson, R. (2016). It's a "Brave" New World... or is it? [Blog post]. Retrieved on 13 February 2021 from https://dfir.blog/its-a-brave-new-world-or-is-it/

[3] Bose, M. (2018). VMware vs. Virtual Box: Comprehensive Comparison [Blog post]. Retrieved on 21 February 2021 from https://www.nakivo.com/blog/vmware-vs-virtual-box-comprehensive-comparison/

[4] Brave. (2021). Brave Rewards. Get rewarded for browsing and support your favorite content creators. Retrieved on 11 March 2021 from https://brave.com/brave-rewards/

[5] Brave Blog. (2021). Brave Passes 25 Million Monthly Active Users [Blog post] Retrieved on 04 March 2021 from https://brave.com/25m-mau/

[6] Crown Prosecution Service (2019). Cybercrime - prosecution guidance. Retrieved on 13 February 2021 from https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

[7] Daniel, E. (2018). Five years on, what has changed since the Edward Snowden scandal?. Retrieved on 20 February 2021 from https://www.verdict.co.uk/snowden-scandal-five-years-gdpr/url

[8] Keizer, G. (2020). Google's Chromium browser explained. Retrieved on 20 February 2021 from https://www.computerworld.com/article/3261009/googles-chromium-browser-explained.html

[9] HMRC. (2016). London ice-cream magnate jailed for £1.6m VAT fraud. Retrieved on 04 March 2021 from https://www.mynewsdesk.com/uk/hm-revenue-customs-hmrc/pressreleases/london-ice-cream-magnate-jailed-for-ps1-dot-6m-vat-fraud-1497890

[10] Jadhav, M., & Meshram, B. (2018). Web Browser Forensics for Detecting User Activities. International Research Journal of Engineering and Technology (IRJET), 05(07), 273-279. Retrieved on 13 February 2021 from https://www.irjet.net/archives/V5/i7/IRJET-V5I748.pdf

[11] Kemp, S. (2020). Digital 2020: July Global Statshot. Retrieved on 13 February 2021 from https://datareportal.com/reports/digital-2020-july-global-statshot

[12] Magnet. (2017). Digital Forensics: Artifact Profile – Google Chrome [Blog post]. Retrieved on 02 March 2021 from https://www.magnetforensics.com/blog/artifact-profile-google-chrome/

[13] Mahlous, A., & Mahlous, H. (2020). Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser. International Journal of Intelligent Engineering Systems, 13(06), 294-306. Retrieved on 20 February 2021 from http://oaji.net/articles/2020/3603-1603767732.pdf

[14] Malviya, N. (2020). Browser Forensics: Google Chrome. Retrieved on 21 March 2021 from https://resources.infosecinstitute.com/topic/browser-forensics-google-chrome

[15] Reed. A, Scanlon. M, & Le-Khac. N-A. (2017) Private Web Browser Forensics: A Case Study of the Epic Privacy Browser. Retrieved on 14 February 2021 from https://arxiv.org/ftp/arxiv/papers/1708/1708.01732.pdf

[16] Shafqat, N. (2016). Forensic Investigation of User's Web Activity on Google Chrome using various Forensic Tools. CSNS International Journal of Computer Science and Network Security, 16(09), 123-132. Retrieved on 20 February 2021 from http://paper.ijcsns.org/07_book/201609/20160919.pdf

[17] StatCounter. (2021a). Browser Market Share Worldwide. Retrieved on 13 February 2021 from https://gs.statcounter.com/browser-market-share

[18] StatCounter. (2021b). Desktop Windows Version Market Share Worldwide. Retrieved on 13 February 2021 from https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

[19] Wilson, C. (2018). Brave. Retrieved on 20 February 2021 from https://kb.digital-detective.net/display/BF/Brave

[20] Berham, Stuart (2021): Appendix A: Supporting Tables and Figures. Cranfield Online Research Data (CORD). Dataset. Retrieved from APPENDIX_A.docx

[21] Nir Sofer. (2021). Nirsoft Tools [Computer Software]. Retrieved from https://www.nirsoft.net/

[22] AccessData. (2017). FTK Imager (v4.1.1.1) [Computer Software]. Retrieved from https://accessdata.com/product-download/ftk-imager-version-4-1-1

[23] X-Ways Software Technology AG. (2021). X-Ways WinHex (v20.1) [Computer Software]. Retrieved from http://www.x-ways.net/winhex/index-m.html

[24] Piacentini, M. et al. (2020). DB Browser for SQLite (v3.12.1) [Computer Software]. Retrieved from https://sqlitebrowser.org/

Appendices

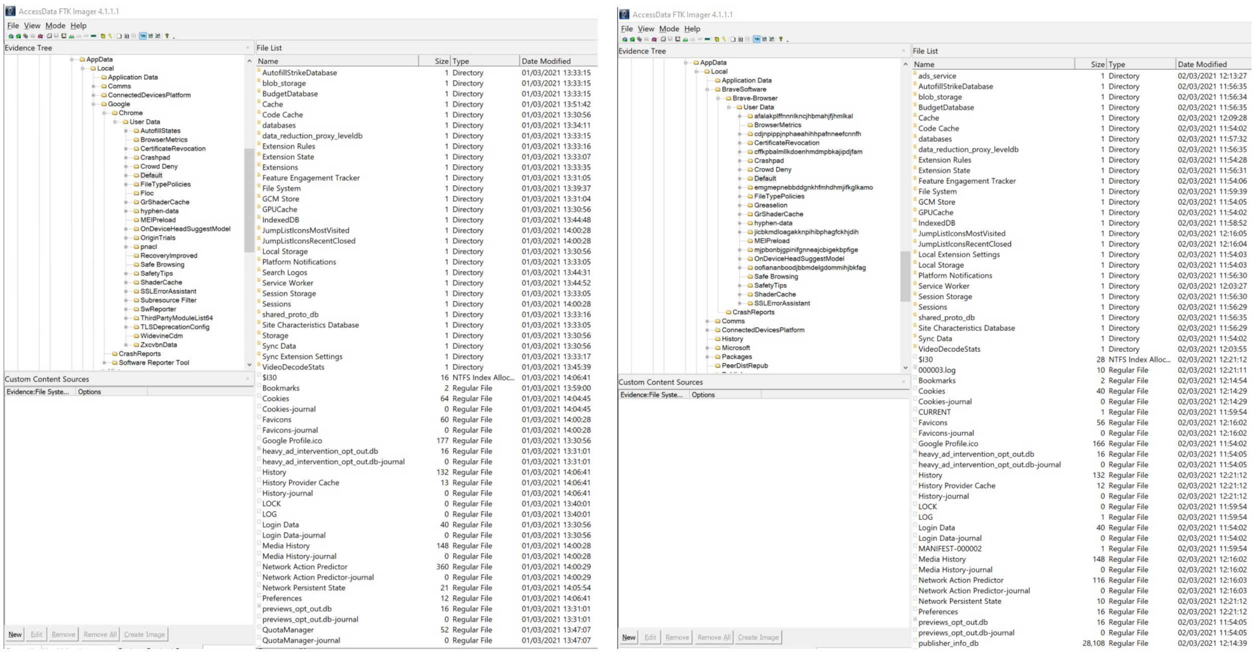
A. SUPPORTING TABLES AND FIGURES

Table A1. Virtual Machine Snapshot Summary

Snapshot	**Browser**	**Description**
Snapshot 1	VM_Base_Image	Windows 10 Installed
Snapshot 2	VM_Base_Image	Installation of VMTools
Snapshot 3 - Google Chrome Installation	Google Chrome	Install of Google Chrome web browser
Snapshot 4 - Google Chrome Opened	Google Chrome	Chrome session opened
Snapshot 5 - Browser Activity	Google Chrome	Completion of user browsing activity
Snapshot 6 - Browser Activity Completed	Google Chrome	Data population and deletion completed
Snapshot 7 - Brower Closed	Google Chrome	
Snapshot 3 - Brave Browser Installation	Brave Browser	Install of Brave Browser
Snapshot 4 - Brave Browser Opened	Brave Browser	Brave session opened
Snapshot 5 - Browser Activity	Brave Browser	Completion of user browsing activity
Snapshot 6 - Browser Activity Completed	Brave Browser	Data population and deletion completed
Snapshot 7 - Browser Closed	Brave Browser	

Table A2. Binary Deconstruction of History DB Record

Record	**Type**	**Data Type**	**Data**	**Table Column Field**
0x84 0x21	Multi-VARINT 1000010000100001 0000001000100001 545-13=532 532/2=266	String	https://consent.google.com/set? continue=https://www.google.co.uk/?gws_rd%3Dssl &origin=https://www.google.co.uk&v=GB.en-GB %2BV9%2BBX%2B227&cc=1&if=1&gl=GB &x=3&pc=s&t1=ADw3F8jqJKAJEdMXZRQ KolkzhAlN4ygGA:1614686769330&t2=ADw3F8i TvaPyG4TKWmRPpNIIlv4dUJrabg:1614686772021	url
0x0D	13-13=0	String		title
0x09	Integer constant 1	Int	1	visit_count
0x08	Integer constant 0	Int	0	type_count
0x06	Big endian 64-bit twos-complement integer	Int	13259160372688846	last_visit_time
0x09	Integer constant 1	Int	1	hidden



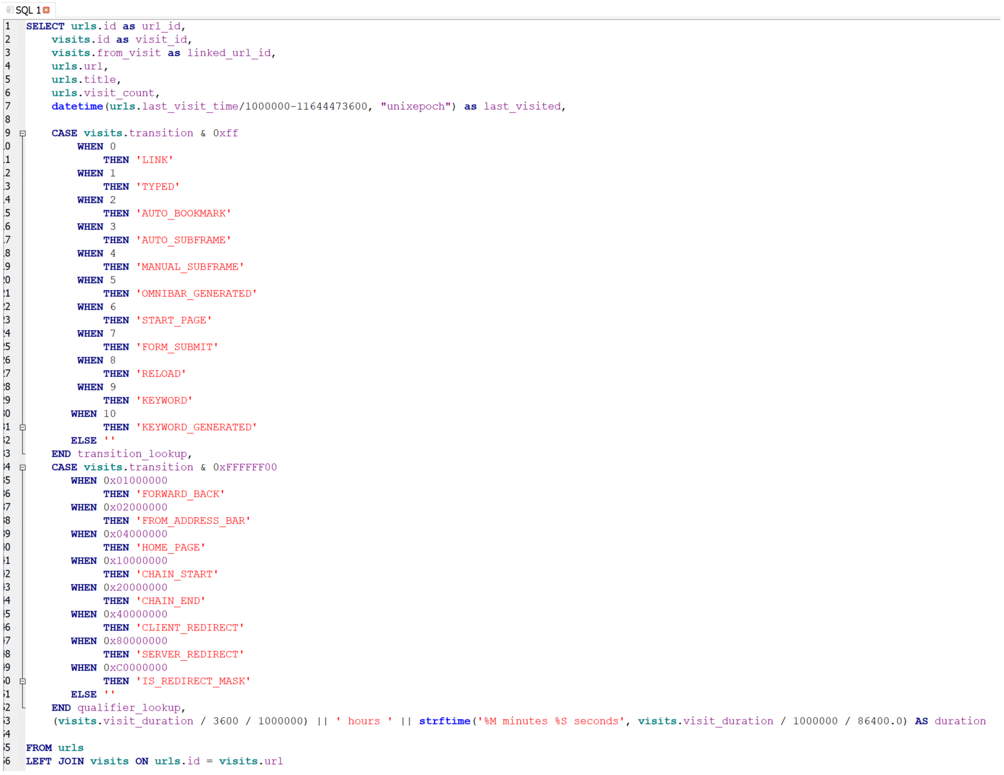
```
AppData
  Local
    Application Data
    Comms
    ConnectedDevicesPlatform
    Google
      Chrome
        User Data
          AutofillStates
          BrowserMetrics
          CertificateRevocation
          Crashpad
          Crowd Deny
          Default
          FileTypePolicies
          Floc
          GrShaderCache
          hyphen-data
          MEIPreload
          OnDeviceHeadSuggestModel
          OriginTrials
          pnacl
          RecoveryImproved
          Safe Browsing
          SafetyTips
          ShaderCache
          SSLErrorAssistant
          Subresource Filter
          SwReporter
          ThirdPartyModuleList64
          TLSDeprecationConfig
          WidevineCdm
          ZxcvbnData
        CrashReports
        Software Reporter Tool
```

Name	Size	Type	Date Modified
AutofillStrikeDatabase	1	Directory	01/03/2021 13:33:15
blob_storage	1	Directory	01/03/2021 13:33:15
BudgetDatabase	1	Directory	01/03/2021 13:33:15
Cache	1	Directory	01/03/2021 13:51:42
Code Cache	1	Directory	01/03/2021 13:30:56
databases	1	Directory	01/03/2021 13:34:11
data_reduction_proxy_leveldb	1	Directory	01/03/2021 13:33:15
Extension Rules	1	Directory	01/03/2021 13:33:16
Extension State	1	Directory	01/03/2021 13:33:07
Extensions	1	Directory	01/03/2021 13:33:35
Feature Engagement Tracker	1	Directory	01/03/2021 13:31:05
File System	1	Directory	01/03/2021 13:39:37
GCM Store	1	Directory	01/03/2021 13:31:04
GPUCache	1	Directory	01/03/2021 13:30:56
IndexedDB	1	Directory	01/03/2021 13:44:48
JumpListIconsMostVisited	1	Directory	01/03/2021 14:00:28
JumpListIconsRecentClosed	1	Directory	01/03/2021 14:00:28
Local Storage	1	Directory	01/03/2021 13:30:56
Platform Notifications	1	Directory	01/03/2021 13:33:05
Search Logos	1	Directory	01/03/2021 13:44:31
Service Worker	1	Directory	01/03/2021 13:44:52
Session Storage	1	Directory	01/03/2021 13:33:05
Sessions	1	Directory	01/03/2021 14:00:28
shared_proto_db	1	Directory	01/03/2021 13:33:16
Site Characteristics Database	1	Directory	01/03/2021 13:33:05
Storage	1	Directory	01/03/2021 13:30:56
Sync Data	1	Directory	01/03/2021 13:30:56
Sync Extension Settings	1	Directory	01/03/2021 13:33:17
VideoDecodeStats	1	Directory	01/03/2021 13:45:39
$I30	16	NTFS Index Alloc...	01/03/2021 14:06:41
Bookmarks	2	Regular File	01/03/2021 13:59:00
Cookies	64	Regular File	01/03/2021 14:04:45
Cookies-journal	0	Regular File	01/03/2021 14:04:45
Favicons	60	Regular File	01/03/2021 14:00:28
Favicons-journal	0	Regular File	01/03/2021 14:00:28
Google Profile.ico	177	Regular File	01/03/2021 13:30:56
heavy_ad_intervention_opt_out.db	16	Regular File	01/03/2021 13:31:01
heavy_ad_intervention_opt_out.db-journal	0	Regular File	01/03/2021 13:31:01
History	132	Regular File	01/03/2021 14:06:41
History Provider Cache	13	Regular File	01/03/2021 14:06:41
History-journal	0	Regular File	01/03/2021 14:06:41
LOCK	0	Regular File	01/03/2021 13:40:01
LOG	0	Regular File	01/03/2021 13:40:01
Login Data	40	Regular File	01/03/2021 13:30:56
Login Data-journal	0	Regular File	01/03/2021 13:30:56
Media History	148	Regular File	01/03/2021 14:00:28
Media History-journal	0	Regular File	01/03/2021 14:00:28
Network Action Predictor	360	Regular File	01/03/2021 14:00:29
Network Action Predictor-journal	0	Regular File	01/03/2021 14:00:29
Network Persistent State	21	Regular File	01/03/2021 14:05:54
Preferences	12	Regular File	01/03/2021 14:06:41
previews_opt_out.db	16	Regular File	01/03/2021 13:31:01
previews_opt_out.db-journal	0	Regular File	01/03/2021 13:31:01
QuotaManager	52	Regular File	01/03/2021 13:47:07
QuotaManager-journal	0	Regular File	01/03/2021 13:47:07

```
AppData
  Local
    Application Data
    BraveSoftware
      Brave-Browser
        User Data
          afalakplffnnnlkncjhbmahjfjhmlkal
          BrowserMetrics
          cdjnpippjnphaeahihhpafnneefcnnfh
          CertificateRevocation
          cffkpbalmllkdoenhmdmpbkajipdjfam
          Crashpad
          Crowd Deny
          Default
          emgmepnebbddgnkhfmhdhmjifkglkamo
          FileTypePolicies
          Greaselion
          GrShaderCache
          hyphen-data
          jicbkmdloagakknpihibphagfckhjdih
          MEIPreload
          mjpbonbjgpinifgnneajcbigekbpfige
          OnDeviceHeadSuggestModel
          oofiananboodjbbmdelgdommihjbkfag
          Safe Browsing
          SafetyTips
          ShaderCache
          SSLErrorAssistant
      CrashReports
    Comms
    ConnectedDevicesPlatform
    History
    Microsoft
    Packages
    PeerDistRepub
```

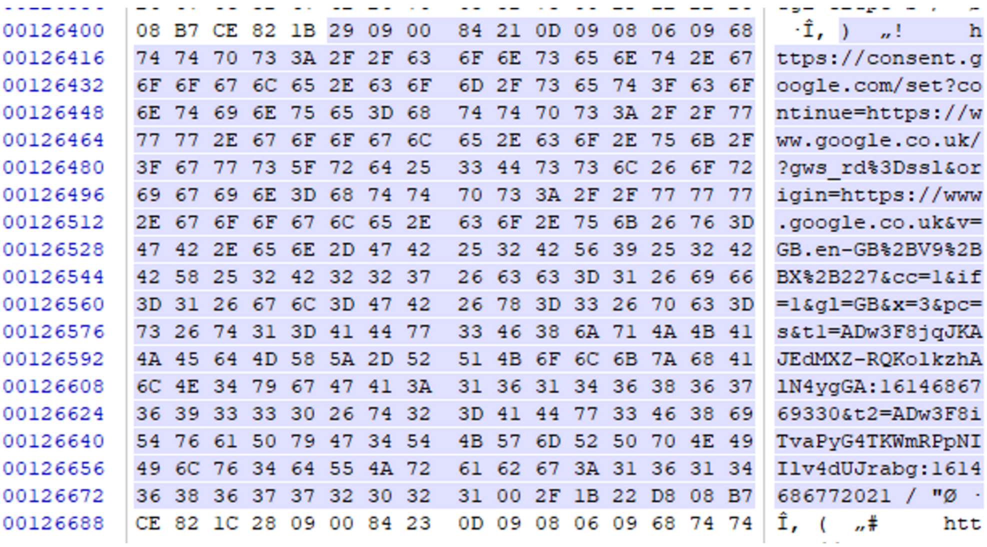
Name	Size	Type	Date Modified
ads_service	1	Directory	02/03/2021 12:13:27
AutofillStrikeDatabase	1	Directory	02/03/2021 11:56:35
blob_storage	1	Directory	02/03/2021 11:56:34
BudgetDatabase	1	Directory	02/03/2021 11:56:35
Cache	1	Directory	02/03/2021 12:09:28
Code Cache	1	Directory	02/03/2021 11:54:02
databases	1	Directory	02/03/2021 11:57:32
data_reduction_proxy_leveldb	1	Directory	02/03/2021 11:56:35
Extension Rules	1	Directory	02/03/2021 11:54:28
Extension State	1	Directory	02/03/2021 11:56:31
Feature Engagement Tracker	1	Directory	02/03/2021 11:54:06
File System	1	Directory	02/03/2021 11:59:39
GCM Store	1	Directory	02/03/2021 11:54:05
GPUCache	1	Directory	02/03/2021 11:54:02
IndexedDB	1	Directory	02/03/2021 11:58:52
JumpListIconsMostVisited	1	Directory	02/03/2021 12:16:05
JumpListIconsRecentClosed	1	Directory	02/03/2021 12:16:04
Local Extension Settings	1	Directory	02/03/2021 11:54:03
Local Storage	1	Directory	02/03/2021 11:54:03
Platform Notifications	1	Directory	02/03/2021 11:56:30
Service Worker	1	Directory	02/03/2021 12:03:27
Session Storage	1	Directory	02/03/2021 11:56:30
Sessions	1	Directory	02/03/2021 11:56:29
shared_proto_db	1	Directory	02/03/2021 11:56:35
Site Characteristics Database	1	Directory	02/03/2021 11:56:29
Sync Data	1	Directory	02/03/2021 11:54:02
VideoDecodeStats	1	Directory	02/03/2021 12:03:55
$I30	28	NTFS Index Alloc...	02/03/2021 12:21:12
000003.log	10	Regular File	02/03/2021 12:21:11
Bookmarks	2	Regular File	02/03/2021 12:14:54
Cookies	40	Regular File	02/03/2021 12:14:29
Cookies-journal	0	Regular File	02/03/2021 12:14:29
CURRENT	1	Regular File	02/03/2021 11:59:54
Favicons	56	Regular File	02/03/2021 12:16:02
Favicons-journal	0	Regular File	02/03/2021 12:16:02
Google Profile.ico	166	Regular File	02/03/2021 11:54:02
heavy_ad_intervention_opt_out.db	16	Regular File	02/03/2021 11:54:05
heavy_ad_intervention_opt_out.db-journal	0	Regular File	02/03/2021 11:54:05
History	132	Regular File	02/03/2021 12:21:12
History Provider Cache	12	Regular File	02/03/2021 12:21:12
History-journal	0	Regular File	02/03/2021 12:21:12
LOCK	0	Regular File	02/03/2021 11:59:54
LOG	1	Regular File	02/03/2021 11:59:54
Login Data	40	Regular File	02/03/2021 11:54:02
Login Data-journal	0	Regular File	02/03/2021 11:54:02
MANIFEST-000002	1	Regular File	02/03/2021 11:59:54
Media History	148	Regular File	02/03/2021 12:16:02
Media History-journal	0	Regular File	02/03/2021 12:16:02
Network Action Predictor	116	Regular File	02/03/2021 12:16:03
Network Action Predictor-journal	0	Regular File	02/03/2021 12:16:03
Network Persistent State	10	Regular File	02/03/2021 12:21:12
Preferences	16	Regular File	02/03/2021 12:21:12
previews_opt_out.db	16	Regular File	02/03/2021 11:54:05
previews_opt_out.db-journal	0	Regular File	02/03/2021 11:54:05
publisher_info_db	28,108	Regular File	02/03/2021 12:14:39

Figure A1. Browser Directory Side by Side Comparison



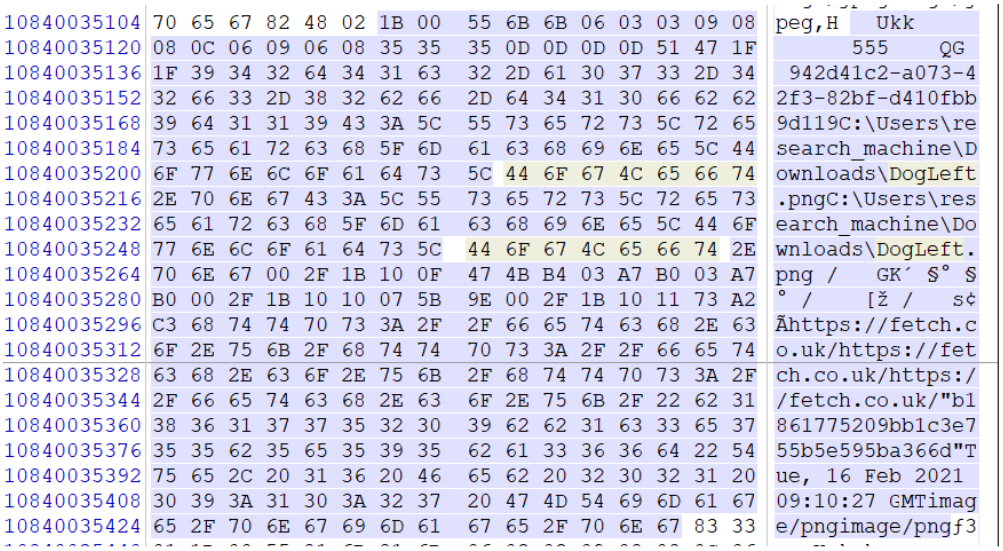
```sql
SELECT urls.id as url_id,
    visits.id as visit_id,
    visits.from_visit as linked_url_id,
    urls.url,
    urls.title,
    urls.visit_count,
    datetime(urls.last_visit_time/1000000-11644473600, "unixepoch") as last_visited,

    CASE visits.transition & 0xff
        WHEN 0
            THEN 'LINK'
        WHEN 1
            THEN 'TYPED'
        WHEN 2
            THEN 'AUTO_BOOKMARK'
        WHEN 3
            THEN 'AUTO_SUBFRAME'
        WHEN 4
            THEN 'MANUAL_SUBFRAME'
        WHEN 5
            THEN 'OMNIBAR_GENERATED'
        WHEN 6
            THEN 'START_PAGE'
        WHEN 7
            THEN 'FORM_SUBMIT'
        WHEN 8
            THEN 'RELOAD'
        WHEN 9
            THEN 'KEYWORD'
       WHEN 10
            THEN 'KEYWORD_GENERATED'
       ELSE ''
    END transition_lookup,
    CASE visits.transition & 0xFFFFFF00
       WHEN 0x01000000
            THEN 'FORWARD_BACK'
       WHEN 0x02000000
            THEN 'FROM_ADDRESS_BAR'
       WHEN 0x04000000
            THEN 'HOME_PAGE'
       WHEN 0x10000000
            THEN 'CHAIN_START'
       WHEN 0x20000000
            THEN 'CHAIN_END'
       WHEN 0x40000000
            THEN 'CLIENT_REDIRECT'
       WHEN 0x80000000
            THEN 'SERVER_REDIRECT'
       WHEN 0xC0000000
            THEN 'IS_REDIRECT_MASK'
       ELSE ''
    END qualifier_lookup,
    (visits.visit_duration / 3600 / 1000000) || ' hours ' || strftime('%M minutes %S seconds', visits.visit_duration / 1000000 / 86400.0) AS duration

FROM urls
LEFT JOIN visits ON urls.id = visits.url
```

Figure A2. History DB SQL Query



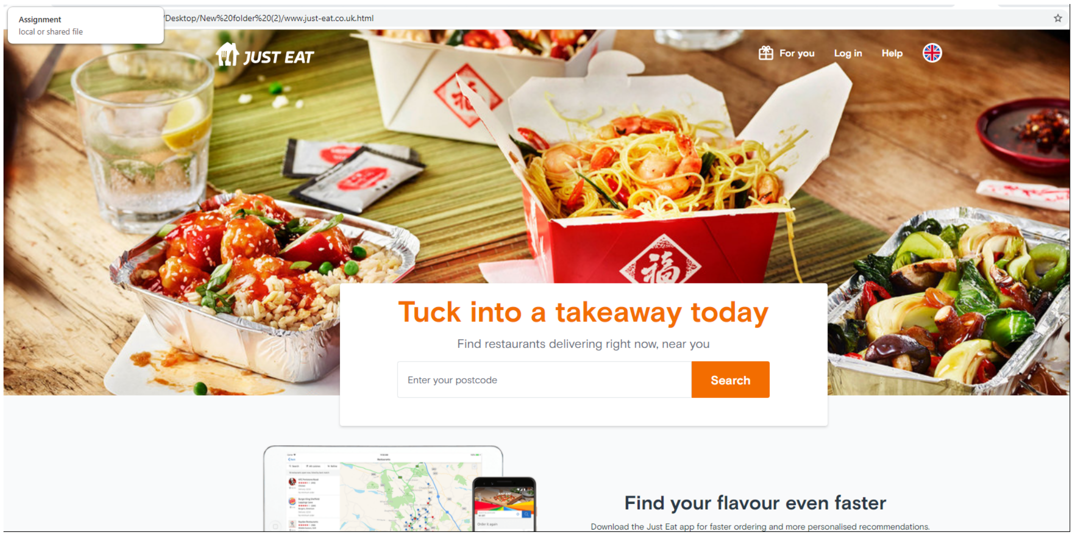
```
00126400  08 B7 CE 82 1B 29 09 00  84 21 0D 09 08 06 09 68   ·Î‚ )  „!     h
00126416  74 74 70 73 3A 2F 2F 63  6F 6E 73 65 6E 74 2E 67  ttps://consent.g
00126432  6F 6F 67 6C 65 2E 63 6F  6D 2F 73 65 74 3F 63 6F  oogle.com/set?co
00126448  6E 74 69 6E 75 65 3D 68  74 74 70 73 3A 2F 2F 77  ntinue=https://w
00126464  77 77 2E 67 6F 6F 67 6C  65 2E 63 6F 2E 75 6B 2F  ww.google.co.uk/
00126480  3F 67 77 73 5F 72 64 25  33 44 73 73 6C 26 6F 72  ?gws_rd%3Dssl&or
00126496  69 67 69 6E 3D 68 74 74  70 73 3A 2F 2F 77 77 77  igin=https://www
00126512  2E 67 6F 6F 67 6C 65 2E  63 6F 2E 75 6B 26 76 3D  .google.co.uk&v=
00126528  47 42 2E 65 6E 2D 47 42  25 32 42 56 39 25 32 42  GB.en-GB%2BV9%2B
00126544  42 58 25 32 42 32 32 37  26 63 63 3D 31 26 69 66  BX%2B227&cc=1&if
00126560  3D 31 26 67 6C 3D 47 42  26 78 3D 33 26 70 63 3D  =1&gl=GB&x=3&pc=
00126576  73 26 74 31 3D 41 44 77  33 46 38 6A 71 4A 4B 41  s&t1=ADw3F8jqJKA
00126592  4A 45 64 4D 58 5A 2D 52  51 4B 6F 6C 6B 7A 68 41  JEdMXZ-RQKolkzhA
00126608  6C 4E 34 79 67 47 41 3A  31 36 31 34 36 38 36 37  lN4ygGA:16146867
00126624  36 39 33 33 30 26 74 32  3D 41 44 77 33 46 38 69  69330&t2=ADw3F8i
00126640  54 76 61 50 79 47 34 54  4B 57 6D 52 50 70 4E 49  TvaPyG4TKWmRPpNI
00126656  49 6C 76 34 64 55 4A 72  61 62 67 3A 31 36 31 34  Ilv4dUJrabg:1614
00126672  36 38 36 37 37 32 30 32  31 00 2F 1B 22 D8 08 B7  686772021 / "Ø ·
00126688  CE 82 1C 28 09 00 84 23  0D 09 08 06 09 68 74 74  Î‚ (  „#     htt
```

Figure A3. History DB Record Binary



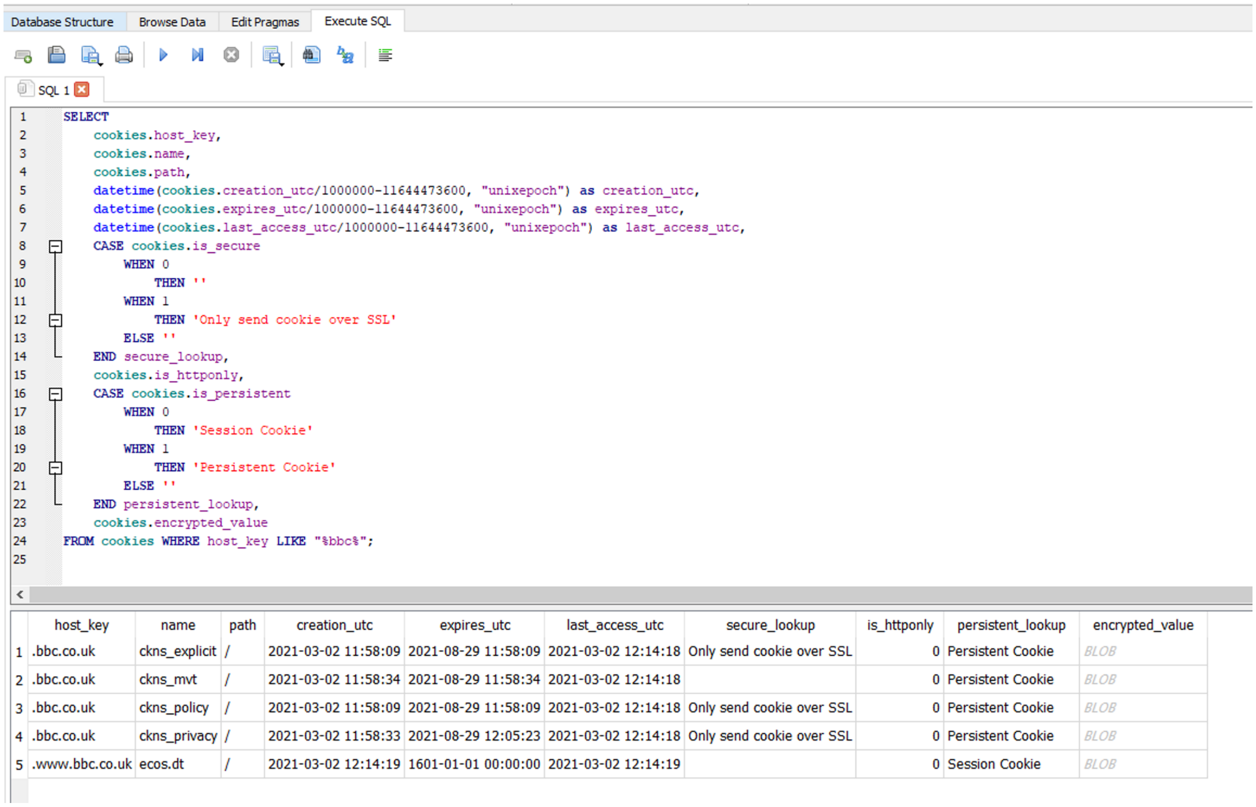
```
10840035104 70 65 67 82 48 02 1B 00  55 6B 6B 06 03 03 09 08 peg,H   Ukk
10840035120 08 0C 06 09 06 08 35 35  35 0D 0D 0D 0D 51 47 1F        555    QG
10840035136 1F 39 34 32 64 34 31 63  32 2D 61 30 37 33 2D 34  942d41c2-a073-4
10840035152 32 66 33 2D 38 32 62 66  2D 64 34 31 30 66 62 62 2f3-82bf-d410fbb
10840035168 39 64 31 31 39 43 3A 5C  55 73 65 72 73 5C 72 65 9d119C:\Users\re
10840035184 73 65 61 72 63 68 5F 6D  61 63 68 69 6E 65 5C 44 search_machine\D
10840035200 6F 77 6E 6C 6F 61 64 73  5C 44 6F 67 4C 65 66 74 ownloads\DogLeft
10840035216 2E 70 6E 67 43 3A 5C 55  73 65 72 73 5C 72 65 73 .pngC:\Users\res
10840035232 65 61 72 63 68 5F 6D 61  63 68 69 6E 65 5C 44 6F earch_machine\Do
10840035248 77 6E 6C 6F 61 64 73 5C  44 6F 67 4C 65 66 74 2E wnloads\DogLeft.
10840035264 70 6E 67 00 2F 1B 10 0F  47 4B B4 03 A7 B0 03 A7 png /   GK´ §° §
10840035280 B0 00 2F 1B 10 10 07 5B  9E 00 2F 1B 10 11 73 A2 ° /    [ž /   s¢
10840035296 C3 68 74 74 70 73 3A 2F  2F 66 65 74 63 68 2E 63 Ãhttps://fetch.c
10840035312 6F 2E 75 6B 2F 68 74 74  70 73 3A 2F 2F 66 65 74 o.uk/https://fet
10840035328 63 68 2E 63 6F 2E 75 6B  2F 68 74 74 70 73 3A 2F ch.co.uk/https:/
10840035344 2F 66 65 74 63 68 2E 63  6F 2E 75 6B 2F 22 62 31 /fetch.co.uk/"b1
10840035360 38 36 31 37 37 35 32 30  39 62 62 31 63 33 65 37 861775209bb1c3e7
10840035376 35 35 62 35 65 35 39 35  62 61 33 36 36 64 22 54 55b5e595ba366d"T
10840035392 75 65 2C 20 31 36 20 46  65 62 20 32 30 32 31 20 ue, 16 Feb 2021
10840035408 30 39 3A 31 30 3A 32 37  20 47 4D 54 69 6D 61 67 09:10:27 GMTimag
10840035424 65 2F 70 6E 67 69 6D 61  67 65 2F 70 6E 67 83 33 e/pngimage/pngƒ3
```

Figure A4. Recovered File Download Database Record



Assignment
local or shared file
/Desktop/New%20folder%20(2)/www.just-eat.co.uk.html
JUST EAT
For you
Log in
Help
Tuck into a takeaway today
Find restaurants delivering right now, near you
Enter your postcode
Search
Find your flavour even faster
Download the Just Eat app for faster ordering and more personalised recommendations.

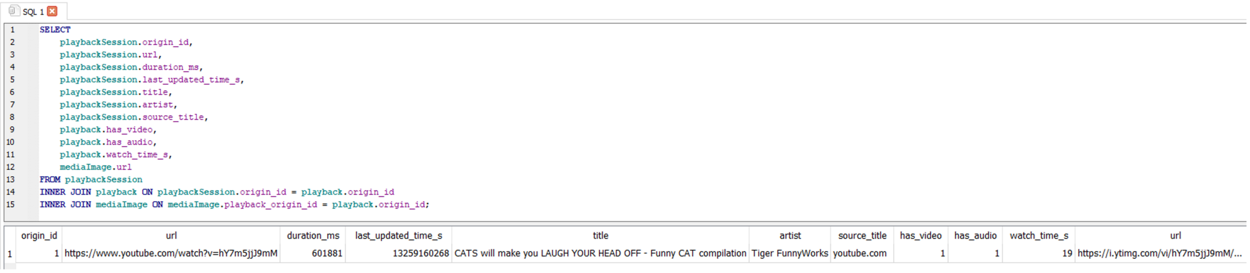
Figure A5. Cached Local Website



```sql
SELECT
    cookies.host_key,
    cookies.name,
    cookies.path,
    datetime(cookies.creation_utc/1000000-11644473600, "unixepoch") as creation_utc,
    datetime(cookies.expires_utc/1000000-11644473600, "unixepoch") as expires_utc,
    datetime(cookies.last_access_utc/1000000-11644473600, "unixepoch") as last_access_utc,
    CASE cookies.is_secure
        WHEN 0
            THEN ''
        WHEN 1
            THEN 'Only send cookie over SSL'
        ELSE ''
    END secure_lookup,
    cookies.is_httponly,
    CASE cookies.is_persistent
        WHEN 0
            THEN 'Session Cookie'
        WHEN 1
            THEN 'Persistent Cookie'
        ELSE ''
    END persistent_lookup,
    cookies.encrypted_value
FROM cookies WHERE host_key LIKE "%bbc%";
```

	host_key	name	path	creation_utc	expires_utc	last_access_utc	secure_lookup	is_httponly	persistent_lookup	encrypted_value
1	.bbc.co.uk	ckns_explicit	/	2021-03-02 11:58:09	2021-08-29 11:58:09	2021-03-02 12:14:18	Only send cookie over SSL	0	Persistent Cookie	BLOB
2	.bbc.co.uk	ckns_mvt	/	2021-03-02 11:58:34	2021-08-29 11:58:34	2021-03-02 12:14:18		0	Persistent Cookie	BLOB
3	.bbc.co.uk	ckns_policy	/	2021-03-02 11:58:09	2021-08-29 11:58:09	2021-03-02 12:14:18	Only send cookie over SSL	0	Persistent Cookie	BLOB
4	.bbc.co.uk	ckns_privacy	/	2021-03-02 11:58:33	2021-08-29 12:05:23	2021-03-02 12:14:18	Only send cookie over SSL	0	Persistent Cookie	BLOB
5	.www.bbc.co.uk	ecos.dt	/	2021-03-02 12:14:19	1601-01-01 00:00:00	2021-03-02 12:14:19		0	Session Cookie	BLOB

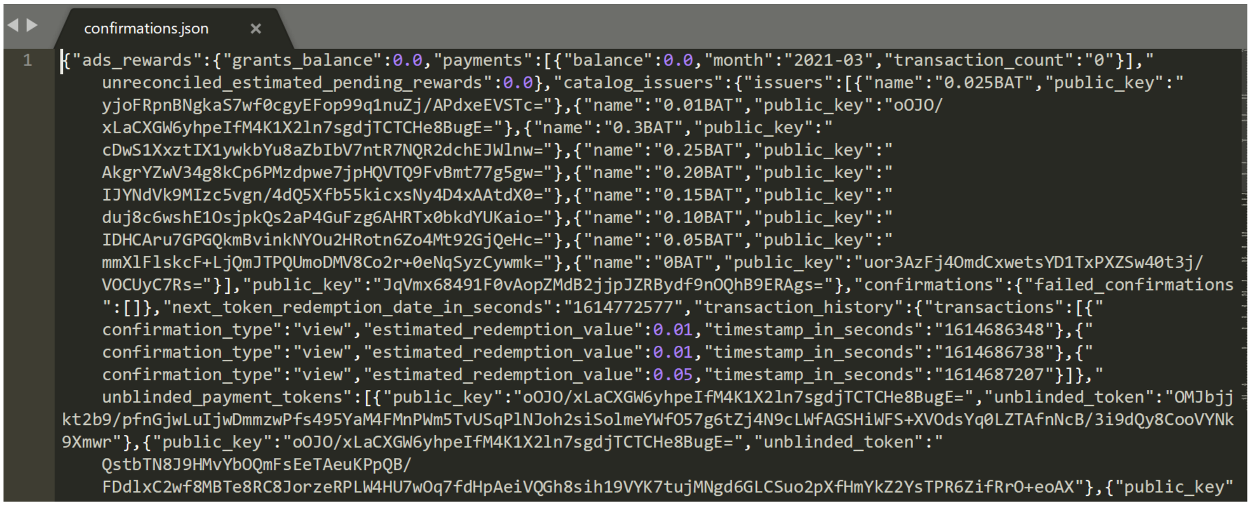
Figure A6. Brave Browser Cookies DB SQL Query



```sql
SELECT
    playbackSession.origin_id,
    playbackSession.url,
    playbackSession.duration_ms,
    playbackSession.last_updated_time_s,
    playbackSession.title,
    playbackSession.artist,
    playbackSession.source_title,
    playback.has_video,
    playback.has_audio,
    playback.watch_time_s,
    mediaImage.url
FROM playbackSession
INNER JOIN playback ON playbackSession.origin_id = playback.origin_id
INNER JOIN mediaImage ON mediaImage.playback_origin_id = playback.origin_id;
```

	origin_id	url	duration_ms	last_updated_time_s	title	artist	source_title	has_video	has_audio	watch_time_s	url
1	1	https://www.youtube.com/watch?v=hY7m5jjJ9mM	601881	13259160268	CATS will make you LAUGH YOUR HEAD OFF - Funny CAT compilation	Tiger FunnyWorks	youtube.com	1	1	19	https://i.ytimg.com/vi/hY7m5jjJ9mM/...

Figure A7. Brave Browser Media History SQL Query



```
{"ads_rewards":{"grants_balance":0.0,"payments":[{"balance":0.0,"month":"2021-03","transaction_count":"0"}],"
    unreconciled_estimated_pending_rewards":0.0},"catalog_issuers":{"issuers":[{"name":"0.025BAT","public_key":"
    yjoFRpnBNgkaS7wf0cgyEFop99q1nuZj/APdxeEVSTc="},{"name":"0.01BAT","public_key":"oOJO/
    xLaCXGW6yhpeIfM4K1X2ln7sgdjTCTCHe8BugE="},{"name":"0.3BAT","public_key":"
    cDwS1XxztIX1ywkbYu8aZbIbV7ntR7NQR2dchEJWlnw="},{"name":"0.25BAT","public_key":"
    AkgrYZwV34g8kCp6PMzdpwe7jpHQVTQ9FvBmt77g5gw="},{"name":"0.20BAT","public_key":"
    IJYNdVk9MIzc5vgn/4dQ5Xfb55kicxsNy4D4xAAtdX0="},{"name":"0.15BAT","public_key":"
    duj8c6wshE1OsjpkQs2aP4GuFzg6AHRTx0bkdYUKaio="},{"name":"0.10BAT","public_key":"
    IDHCAru7GPGQkmBvinkNYOu2HRotn6Zo4Mt92GjQeHc="},{"name":"0.05BAT","public_key":"
    mmXlFlskcF+LjQmJTPQUmoDMV8Co2r+0eNqSyzCywmk="},{"name":"0BAT","public_key":"uor3AzFj4OmdCxwetsYD1TxPXZSw40t3j/
    VOCUyC7Rs="}],"public_key":"JqVmx68491F0vAopZMdB2jjpJZRBydf9nOQhB9ERAgs="},"confirmations":{"failed_confirmations
    ":[]},"next_token_redemption_date_in_seconds":"1614772577","transaction_history":{"transactions":[{"
    confirmation_type":"view","estimated_redemption_value":0.01,"timestamp_in_seconds":"1614686348"},{"
    confirmation_type":"view","estimated_redemption_value":0.01,"timestamp_in_seconds":"1614686738"},{"
    confirmation_type":"view","estimated_redemption_value":0.05,"timestamp_in_seconds":"1614687207"}]},"
    unblinded_payment_tokens":[{"public_key":"oOJO/xLaCXGW6yhpeIfM4K1X2ln7sgdjTCTCHe8BugE=","unblinded_token":"OMJbjj
kt2b9/pfnGjwLuIjwDmmzwPfs495YaM4FMnPWm5TvUSqPlNJoh2siSolmeYWfO57g6tZj4N9cLWfAGSHiWFS+XVOdsYq0LZTAfnNcB/3i9dQy8CooVYNk
9Xmwr"},{"public_key":"oOJO/xLaCXGW6yhpeIfM4K1X2ln7sgdjTCTCHe8BugE=","unblinded_token":"
    QstbTN8J9HMvYbOQmFsEeTAeuKPpQB/
    FDdlxC2wf8MBTe8RC8JorzeRPLW4HU7wOq7fdHpAeiVQGh8sih19VYK7tujMNgd6GLCSuo2pXfHmYkZ2YsTPR6ZifRrO+eoAX"},{"public_key"
```

Figure A8. Brave Attention Token (BAT) Transaction Balance