Original Article

Check for updates

Protecting Digital Footprints: A Selective Web History Sanitization Tool for Domestic Violence Survivors

Rozha Kamal Ahmed[a b *] 🆔 **, Silvia Lips** [b] 🆔 **, Zryan Najat Rashid** [c] 🆔

[a] Network Department, Computer Science Institute, Sulaimani Polytechnic University, Sulaymaniyah, Iraq.
[b] Department of Software Science, School of Information Technologies, Tallinn University of Technology, Tallinn, Estonia.
[c] Computer Networks Department, Technical College of Informatics, Sulaimani Polytechnic University, Sulaymaniyah, Iraq.

Abstract: Survivors of domestic abuse often face significant risks when accessing critical online resources as digital footprints can be monitored by abusive partners, potentially leading to further harm. To address this issue, this research introduces an innovative solution designed to protect the privacy of domestic violence survivors when they are seeking online support without leaving digital traces that could expose them to danger. The proposed system employs the principles of the design science framework, ensuring a structured approach to development and evaluation. It focuses on selective web browsing history sanitization, a novel technique that selectively removes traces of visits to support-related websites while preserving unrelated browsing history. By maintaining an appearance of normal online activity, this system minimizes the risk of arousing suspicion from abusers, striking a careful balance between privacy, security, and usability. A key contribution of this study is the development of an artifact that directly addresses a pressing societal challenge—empowering domestic violence survivors with a secure, adaptive, and user-friendly digital tool to allow them to seek online support with confidence. This is unlike conventional privacy solutions that may require technical skills or indiscriminately erase the entirety of the browsing history. Beyond the advantages of the system to survivors, this research also provides valuable insights for organizations and advocacy groups that support victims of domestic violence. It highlights the importance of privacy-centric digital services and encourages the development of tools and best practices that prioritize user safety. This work contributes to a broader effort to create a safer digital environment for vulnerable populations.

1. Introduction

Internet technologies have made accessing information and services easier worldwide. While these advancements benefit many people, they also pose challenges, particularly in the context of domestic violence. Currently, the majority of domestic violence organizations use websites to provide support and education, allowing survivors to seek help at any time and from any location [1–4] . However, the internet can also have a detrimental impact, particularly through intimate partner cyberstalking, a dominating behavior that threatens the survivors' safety and social well-being [1–7]. To access internet services, survivors frequently use web browsers, which save data such as browsing history, cache, and cookies for faster access. Unfortunately, these features can expose survivors to tracking by abusers [8–12]. Since survivors may lack technical expertise, hiding traces of their activity, such as visits to support websites, becomes a significant challenge [1–3, 7].

To address this significant social challenge and protect survivor privacy, this study adopts the principles of the design science framework as a research approach [13–16]. Accordingly, the aim of this research is to answer the research question, "How can survivors of domestic violence maintain their privacy while obtaining online support?" To answer the research question, the authors' objective is to develop a novel solution with a selective history sanitization agent to help domestic violence survivors safely access support websites. The system will selectively erase traces of visited support sites while preserving other browsing data to avoid suspicion and prevent tracking by abusers.

This article is structured according to the design science research study schema presented by Gregor and Hevner [15]. The Introduction section presents the goal of the artifact to be developed, followed by Section 2 that outlines the research background and provides context and foundational insights based on the analysis of the relevant literature. Section 3 details the methodology employed for the application's development, while Section 4 presents the main results of the study; it details the artifact description, evaluates the artifact, and demonstrates its quality and efficacy. Section 5 offers a discussion of the findings, which also presents reflections on the study's limitations and future research directions, along with the theoretical and practical implications of the findings, showing the significance of the research and its contribution to the knowledge base, followed by concluding remarks in Section 6.

2. Related Works

2.1. Domestic Violence and Cyberstalking

Cyberstalking is typically defined as controlling or harassing behavior using information and communication technologies, which is frequently committed by a partner either during or after a relationship ends, which is highlighted as an important risk factor in domestic violence [1,2, 4–7]. Studies have highlighted the deep harmful effects of domestic violence and cyberstalking on survivors' social lives, emphasizing the serious risks these practices have in relation to their safety and well-being, including feelings of stress, decreasing their quality of life, and psychological harm [17] that could lead to more complicated issues such as losing personal protection and changes in social habits [1, 4, 6]. Stalking is a form of gender-based violence that affects every community, and statistics reveal that one in every three women and one in every six men will experience stalking throughout their lifetime [18].

Cyberstalking is an emerging global concern that threatens the safety, privacy, and well-being of millions worldwide. The Global Kaspersky report published data from 2023 that revealed that stalkerware, surveillance software that domestic abusers secretly employ to monitor their victims, has infected nearly 31,000 mobile users worldwide. In addition to stalkerware, 40% of individuals globally have reported experiencing stalking or suspecting that they were being stalked [19]. In 2024, statistics from England and Wales indicate that stalking has affected one in seven individuals aged 16 and older, with women and younger individuals being disproportionately affected [20]. Furthermore, and similar to other countries, cyberstalking is becoming a widespread problem in the United States, affecting an estimated 7.5 million individuals each year [21]. It is noted that 80% of stalking victims are monitored using technological tools such as mobile phones, text messages, and emails, while 67% are stalked in person. It is worth pointing out that despite the impact of cyberstalking, only 29% of cyberstalking victims in the United States report these offenses to the police [21].

This data clearly highlights the importance of greater preventive measures and accessible support tools as digital services for victims, as well as increased awareness. Reporting processes must be enhanced so then victims are able to seek help from supportive organizations with confidence and without fear of any repercussions.

2.2. Digital Footprints on Web Browsers

2.2.1. Web Browsers

A web browser is a software application that enables users to access, retrieve, and engage with content on the internet; it facilitates the presentation of web pages, photos, videos, and other multimedia content on the internet [11, 22–25]. Some popular web browser examples are Google Chrome,

Mozilla Firefox, and Microsoft Edge, among others. In addition to browsing, web browsers offer other functionalities such as bookmarking, history tracking, and add-ons to improve the user experience [11], [23, 24, 26]. Browsers support storing information and recording visited sites for the purpose of faster retrieval for the next visit; hence, a user's digital footprints can be found and retrieved from the logs of stored information through visited URLs, which are stored in history lists, cache files, cookies, search terms, and others; issues such as the security and privacy of users that are associated with these browsers should be considered carefully [11, 22–24, 27–31]. In particular, users who are not technical savvy, specifically domestic violence survivors, which is the focus of this research.

Based on an in-depth analysis conducted on browsers, the authors found that users' digital footprints are often stored in the following locations:

- **History list**: According to Mugisha [24] and Anuradha *et al.* [25], the history list is a feature for recording and tracking visited webpages where the visit time and Uniform Resource Location (URL) are stored in the computer memory. Generally, browsers allow history lists to be displayed along with the functionality to clear the history list. The format and location of the history list differs from one browser to another.
- **Cache**: According to Mugisha [24] and Anuradha *et al.* [25], the cache is a temporary storage location in the memory used to store copies of many files downloaded from the internet. When URLs are visited, copies of pages are stored to allow the faster retrieval of the visited pages on subsequent visits without downloading them again. Accordingly, the cache serves as a second history to keep a digital footprint of activities. However, there is no simple way to represent its contents. The cache contents are removed after a certain amount of time when space is required for new pages; information stored in the cache is deleted when it is no longer valid. Cache contents can also be manually removed, as all modern browsers provide features for clearing or emptying the cache. Similar to the history list, browsers use different approaches to store the cache, which is kept in different locations.
- **Cookies**: According to some studies [11, 12, 24, 25], cookies are saved files on local computers (client computers). They are generated by the web servers when users are visiting websites. The cookies file stores information about the login used, such as the domain name and date/time stamps. Cookies are stored differently in different browsers.
- **Bookmark**: According to Anuradha *et al.* [25], a bookmark is a feature provided by browsers to allow users to save their favorite webpages for faster later retrival without having to remember the exact address of the URL. Each browser implements and stores the bookmark or favorited pages differently.
- **Domain Name System**: Domain Name System (DNS) is a naming system used on the internet to translate domain names into internet protocol (IP) addresses. It provides a table of the mappings between host names and IP addresses; therefore, visited pages can be cached for future use and retrieved through the DNS cache. DNS content can be accessed on the users' computers locally using the ipconfig/displaydns command in the command line.
- **Downloads**: According to Mugisha [24] and Anuradha *et al.* [25], the downloads folder is used to store downloaded content on the user's computer locally.
- Other potential locations for finding a digital footprint include searched keywords, visited pages that are displayed on the browser interfaces, and typed URLs [24].

2.2.2. *Safe Browsing*

Browsers have implemented private browsing modes with the primary goal of protecting their user's privacy by making their activities intractable during the private session. Private browsing mode aims to not leave the users' digital footprint on the visited websites and to leave no evidence on local computers such as browsing history and cache files, in addition to allowing users to browse websites without revealing their identity [3, 22–24, 32, 33].

Private browsing mode feature was initially introduced in 2005 by the Apple Safari browser. Later, it was added to other browsers such as Google Chrome in 2008, Mozilla Firefox in 2009, and Internet Explorer in 2009, updated to Microsoft Edge in 2015 [22].

Currently, all major browsers support private browsing mode. However, the implementation of privacy protections varies across platforms, and some inconsistencies remain in how browsing activities are handled and stored. Each browser names this feature differently; for instance, it is called "InPrivate Browsing" in Internet Explorer (Microsoft Edge), "Private Browsing" in Firefox Mozilla, and " Incognito" in Google Chrome [32, 33].

While the private mode is aimed at allowing safe browsing without leaving behind a digital footprint about user's online activities, numerous studies have showed that private browsing only affects the application layer that the operating system recognizes. Records of activities can still be recovered and retrieved from the computer's hard disk and random access memory (RAM) where information is stored in the "Pagefile.sys file", using tools such as "MagnetRAMCapture" [24], and the Forensic Tool Kit (FTK) [23]. Rraces of visited sites can also be found in the DNS resolver cache. Therefore, by examining the DNS cache, evidence of visited sites can be found [22, 34]. Furthermore, private mode does not support bookmarks; hence, saving sites in the bookmarks during private sessions can be seen after exiting the private mode.

2.3. Strategies to Support Survives of Domestic Violence

Relevant literature has explored several technological tools used to ensure users' privacy during online activities. Some studies considered private browsing mode as a proper solution to protect users' privacy as it does not involve the browsing history and aims to leave no traces behind when the browsing sessions are ended [22, 23, 32]. Furthermore, Emms *et al.* [7] proposed an improved solution involving browsers with private mode features that can be used through portable devices such as USB or DVDs, and how they tend to provide effective privacy protection when used correctly, but only when the user has technical proficiency as it relies on users remembering to activate and use it properly. Bou Abdo and Zeadally [28] proposes a client-side method that aims to provide layers of anonymization to serve as temporary identities to be used while browsing. The proposed solution allows the user to configure the preferred level of personal privacy. The onion router (TOR) browser explored in the study by Kumar *et al.* [35] uses onion routing to provide access to highly encrypted private modes and anonymizes the web traffic. It also hides users identities. While TOR is essential for privacy, it is frequently used for crimes, such as cyberterrorism and black market activities. Hammoud and Tarkhanov [26] developed a browser extension (browser-level plug-in) that can effectively protect users' privacy across various websites.

When it comes to protecting the privacy of survivors of domestic violence, the analysis of the literature has revealed that relatively little attention has been paid to this subject. In this regard, Arief *et al.* [4] proposed a solution to selectively erase entries from mobile phones, where the proposed solution aims to function on cellphones only with Andriod operating systems. Emms *et al.* [7] proposed two technology-driven solutions to improve survivors' access to domestic violence support websites and to protect their privacy doing so.

- Raising awareness through technologies enhances the accessibility of support services by ensuring that survivors are aware of available support resources. This approach can be achieved through the implementation of quick response codes, as well as near field communication and radio frequency identification tags that can encode a URL or SMS text message and be readable by a smartphone or a laptop with a webcam. This can ensure the dissemination of support organization's web pages. This method should be embedded in an innocent-looking postcard or impage.
- Erasing the digital footprints of survivors after accessing supportive webpages. There are different complementary technologies able to provide layers of protection. For instance, the first approach is to hide domestic violence supportive webpages behind "innocent" pages from legitimate websites that survivors often use to prevent abusers from tracing their browser

history to support pages. The second approach is developing a tool to automatically erase the digital footprints left behind when a survivor accesses specific support websites by selectively removing all history entries related to the support websites. This approach can be implemented on personal computers as well as on cellphones when the survivors seek help through text messages and phone calls.

To summarize, the analysis of related work has provided an overview of numerous solutions for protecting user privacy while browsing [22, 23, 26, 28, 32, 35, 36]. None are specifically designed for domestic violence survivors, and the majority of the proposed methods require technical skills to be able to use them properly.

On the other hand, while Emms *et al.* [7] explored technology-based techniques to support survivors of domestic violence, it provides only a marginal preview of solutions, lacking a detailed technical explanation, implementation and testing of each solution. This study addresses this critical gap by introducing a targeted history sanitization agent specifically designed to support domestic violence survivors in safely accessing digital resources.

3. Materials and Methods

Design science has been reported as a research methodology focused on creating and evaluating IT artifacts intended to solve identified organizational problems [13-16, 37]. Such artifacts may include models, methods, constructs, instantiations (software), social innovations, or new properties of technical, social, or informational resources. Any designed object providing a solution to an identified research problem qualifies as an artifact [13, 15, 16], which significantly contributes to the knowledge base.

Hevner *et al.* [13] have provided a precise research framework for building information systems in the context of the design science approach. Figure 1 illustrates the interaction between the environment, information systems research, and knowledge base to ensure both rigor and relevance. The environment represents people, organizations, and technology, which identify the business needs that drive the research process. The knowledge base is compromised of the foundations that could be theories, models, frameworks, and methodologies as the validation criteria to provide the necessary rigor for the research.
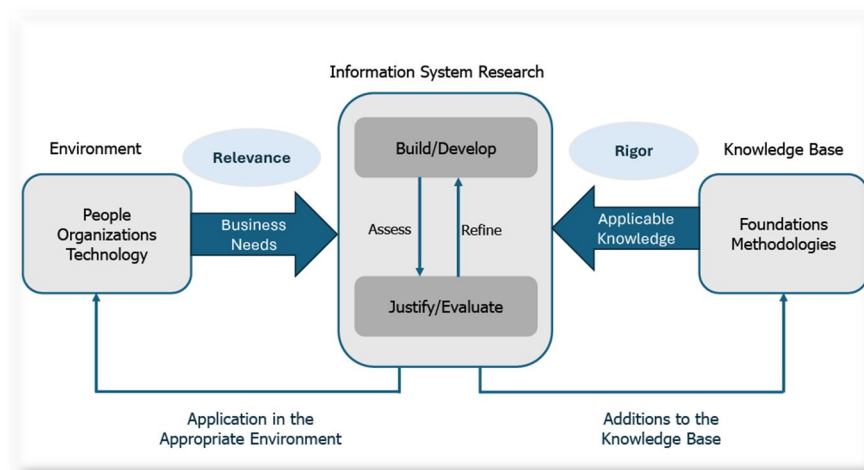
Figure 1: Research framework adapted from Hevner *et al.* [13].

Within the design science framework, the primary focus of the research is focused on two key activities: developing an artifact and rigorously evaluating it through continuous assessment and

refinement while contributing to the knowledge base and ensuring that the final developed artifact addresses the real-world problem effectively [13, 15, 16].

The artifact to be developed in the context of this research is an agent that automatically deletes the digital footprints left behind when a survivor accesses specific domestic violence support websites through web browsers. The agent will automatically remove all history entries related to domestic violence support websites while leaving intact all other history entries to avoid raising the abuser's suspicion.

- For the artifcat development, the authors implemented the system, employing the Agile methodology [38-40], allowing iterative and incremental improvements through constant feedback and modification. This methodology ensures adaptability to changing requirements and promotes the delivery of a high-quality solution that effectively addresses the identified problem.

   As an implementation scope, Mozilla Firefox and Google Chrome web browsers were the primary focus of this project. As there are a wide range of browsers available, it was challenging to extend the analysis to include all browsers. However, the authors are planning to expand the solution to include other popular browsers in the future.

- For the technological tools, C# was selected as the programming language for system development due to its versatility in supporting both web and standalone applications, while it is also considered a robust tool for building Windows applications with reduced coding efforts through various built-in functions. The SQLite database was selected as the databse. According to research into the history lists of Mozilla Firefox and Google Chrome, both browsers store the majority of their history data in modifiable SQLite database files. Artifact description is presented in Section 4.

- For the artifact evaluation, the authors conducted rigorous testing cycles to verify the system's reliability, validity, and efficacy. These efforts were conducted to ensure that the final output properly addresses the study's research question. Artifact evaluation is presented in Section 4.

4. Results

4.1. System Design and Implementation

In the context of the design science framework, this section presents the artifact description.

4.1.1. Target Locations to be Selectively Cleaned

The cleaning functionality was carefully designed to delete only records related to domestic violence support websites, ensuring that other entries remain intact to avoid suspicion by abusers. A list of sample websites was predefined and stored in a separate flat file (text file). This file is referenced during the cleaning process. When the cleaning function is called, the system attempts to connect to the remote file. Depending on the success of the connection, it loads the data from the file as presented in figure 2. For greater efficiency, it was decided to host the file on a server or remote page, allowing updates to be dynamically loaded. Additionally, to mitigate potential server connection issues, a local backup copy is also maintained, ensuring reliable access to the list under all circumstances.
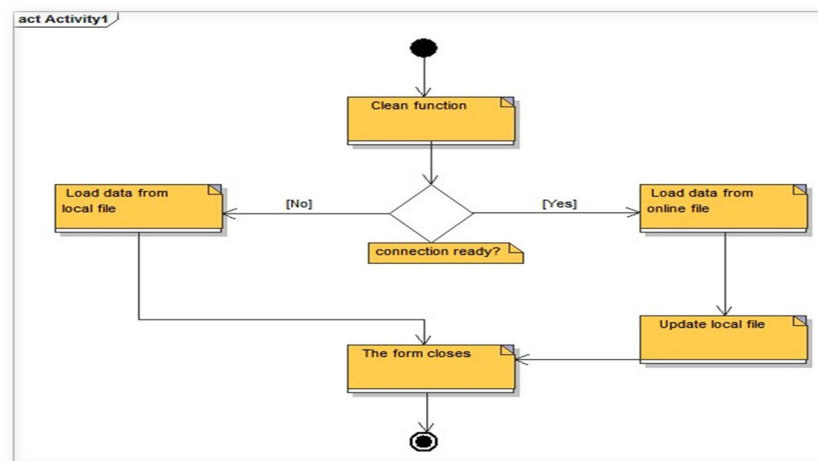
Figure 2: Clean function process modeling.

Upon the successful retrieval of the file, the system compares the history entries with the list and deletes any corresponding records (see section 4.1.2). Table 1 presents an analysis of the identified target locations for the Firefox browser, While table 2 presents an analysis of the identified target locations for the Chrome browser.

Table 1: Target locations in the Firefox browser.

Target locations	Format	Location	Editable directly
History list	SQLite files	moz_places and moz_historyvisits which can be accessed at: C:\Users\<UserName> \App Data\Roaming \Mozilla\Firefox \Profiles \xxxxxxxx.default \places.sqlite	through SQLite database or API's
Cache	binary file format	C:\Users\<UserName>\AppData\Local\Mozilla\Firefox\Profiles \xxxxxxxx.default\Cache C:\Users\<UserName>\AppData\Local\Mozilla\Firefox\Profiles \xxxxxxxx.default\OfflineCache	No
Cookies	SQLite files	moz_cookies table which can be accessed at: C:\Users\<UserName>\AppData\Roaming\Mozilla\Firefox\Profiles \ xxxxxxxx.default\cookies.sqlite	through SQLite database or API's
Bookmarks	SQLite files	moz_bookmarks in places.sqlite database which can be found at: C:\Users\<UserName>\AppData\Roaming\Mozilla\Firefox\Profiles \ xxxxxxxx.default\places.sqlite	through SQLite database or API's
DNS	Zone file	ipconfig/displaydns through the command line on the personal computers locally	No
Downloads	Normal readable folder	C:\Users\[User Name]\Downloads	Yes
Searched keywords	SQLite files	moz_keywords in places.sqlite database which can be found at: C:\Users\<UserName>\AppData\Roaming\Mozilla\Firefox\Profiles \ xxxxxxxx.default\places.sqlite	through SQLite database or API's
Visited pages	SQLite files	moz_inputhistory in places.sqlite database which can be found at: C:\Users\<UserName>\AppData\Roaming\Mozilla\Firefox\Profiles \ xxxxxxxx.default\places.sqlite	through SQLite database or API's
Typed URLs	SQLite files	moz_inputhistory in places.sqlite database which can be found at: C:\Users\<UserName>\AppData\Roaming\Mozilla\Firefox\Profiles \ xxxxxxxx.default\places.sqlite	through SQLite database or API's

Table 2: Target locations in the Chrome browser.

Target locations	Format	Location	Editable directly
History list	SQLite files	History tables which can be accessed at: C:\Users\<UserName> \App Data\Local \Google\Chrome \User Data\Default \History	through SQLite database or API's
Cache	binary file format	C:\Users\<UserName>\AppData\Local\Google\Chrome\UserData\ Default\Cache	No
Cookies	SQLite files	Cookies table which can be accessed at: C:\Users\<UserName>\AppData\Local\Google\Chrome\UserData \Default\Cookies	through SQLite database or API's
Bookmarks	JSON file	Bookmarks and Bookmarks.bak which can be found at: C:\Users\<UserName>\AppData\Local\Google\Chrome\UserData\ Default \Bookmarks C:\Users\<UserName>\AppData\Local\Google\Chrome\UserData\ Default \Bookmarks.bak	No
DNS	Zone file	ipconfig/displaydns through the command line on the personal computers locally	No
Downloads	Normal readable folder	C:\Users\[User Name]\Downloads	Yes
Searched keywords	SQLite files	keyword_search_terms table which can be accessed at: C:\Users\<UserName> \App Data\Local \Google\Chrome \User Data\Default \ History	through SQLite database or API's
Visited pages	SQLite files	Visits table which can be accessed at: C:\Users\<UserName> \App Data\Local \Google\Chrome \User Data\Default \ Visits	through SQLite database or API's
Typed URLs	SQLite files	urls table which can be accessed at: C:\Users\<UserName> \App Data\Local \Google\Chrome \User Data\Default \Urls	through SQLite database or API's

4.1.2. Implementing the System

The implementation stage was carefully planned and allocated sufficient time, with well-structured cycles for development. Special attention was given to error handling by incorporating appropriate exceptions to ensure that the system could manage the various actions effectively and robustly.

Figure 3 presents a high-level explanation of the classes using the Unified Modeling Language (UML) class diagram.
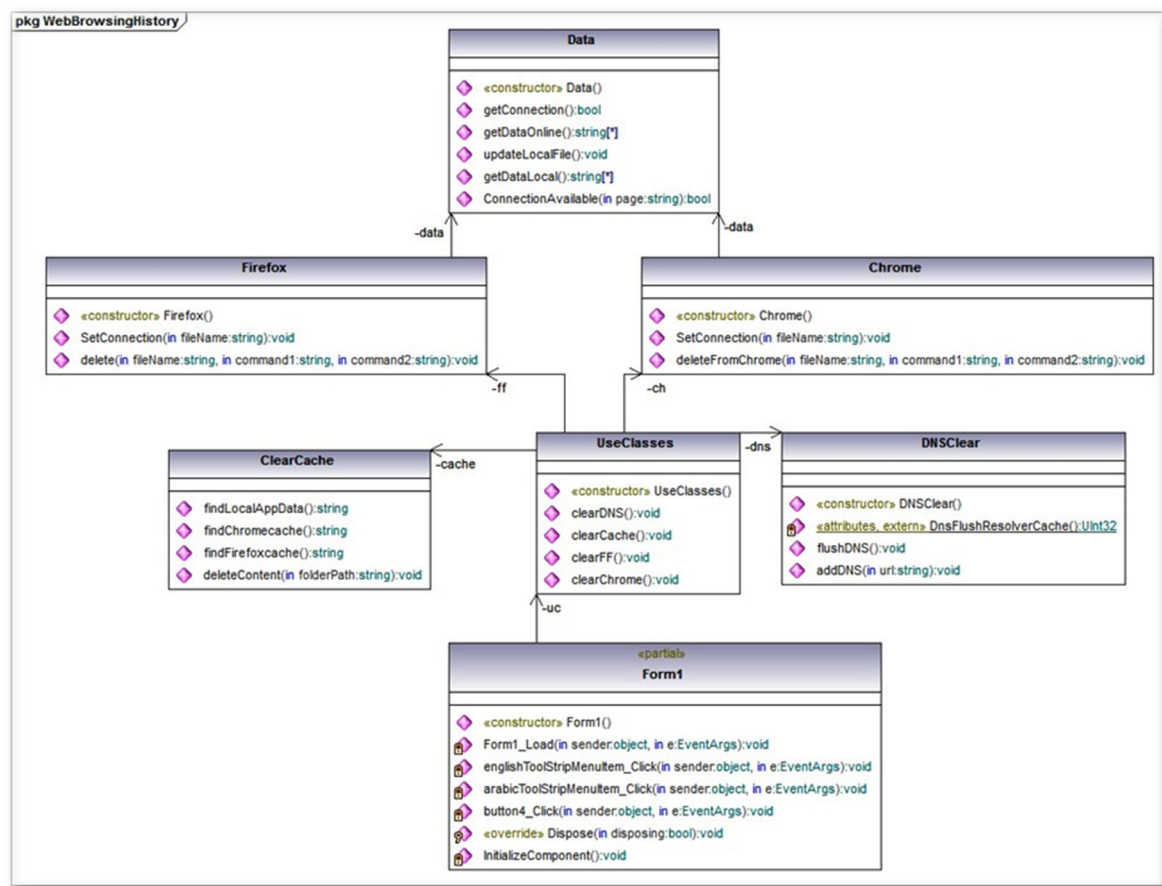
Figure 3: High-level explanation of the classes.

For cleaning actions, the Data class decides which entries to remove. It uses a file system to store deleted sites and synchronize remote and local copies for consistency. The class effectively imports and outputs data using StreamReader and StreamWriter APIs, and is designed for future modifications. After uploading remote modifications, the system updates the local copy. The list of domestic violence support websites store just the site names (e.g., angelou-centre) instead of URLs to ensure comprehensive deletion across the relational tables.

The Firefox class handles connecting to SQLite database files, ensuring that all relational tables are updated to remove traces of deleted sites. The user's profile directory is located within the application data folder by an algorithm that employs built-in C# functions to search its subdirectories for SQLite files.

```
 appData= Environment.GetFolderPath
(Environment.SpecialFolder.ApplicationData);
        //Then if this directory exists, find all SQLite files
        if (Directory. Exists (appData))
         { string[] files = Directory.GetFiles
        (appData, "*.sqlite", SearchOption.AllDirectories); }
```

The Chrome class functions similarly to the Firefox class but is adapted to account for the different storage locations of Google Chrome's database files. Since these records are stored in the local application data directory, the following approach was implemented:

```
ChromeLocalAppData =Environment.GetFolderPath
        (Environment.SpecialFolder.LocalApplicationData);
        string filePath = ChromeLocalAppData +
        \\Google\\Chrome\\UserData\\Default\\;
```

The ClearCache class manages the cache contents for Mozilla Firefox and Google Chrome, which are stored in binary format, not SQLite files. It includes methods to locate cache directories and use loops to delete their contents, including subdirectories, leveraging the DirectoryInfo API.

```
DirectoryInfo cacheInfo = new DirectoryInfo(folderPath);
foreach (FileInfo file in cacheInfo.GetFiles())
  {
    file.Delete();
  }
foreach (DirectoryInfo dir in cacheInfo.GetDirectories())
  {
    dir.Delete(true);
  }
```

Class DNSClear will implement the DNS cleaning history of the stored records. However, to avoid suspicion, it is designed in such a way that by default, the DNS records will be reconstructed. For instance, calling on the method below with different domains as the parameters will send new domain names to the DNS cache.

```
Dns.addDNS("http://www.google.com/");
```

The UseClasses class integrates and manages the functionality of all other classes.
The Form1 class handles the user interface, connecting the functionality to the provided button(s).

The developed artifact aimed at empowering survivors of domestic violence by providing secure access to support websites while leaving no digital footprints. The system was developed for fulfilling survivors' needs with a simple user-friendly and intuitive interface that included plain text and helpful icons for the end user's convenience. The implemented features are presented in Table 3.

Table 3: Implemented features.

No.	Implemented features (Selective cleaning)	Mozilla Firefox	Google Chrome
1	History list	◎	◎
2	Cache	deletes all entries	deletes all entries
3	Cookies	◎	◎
4	Bookmarks	◎	◎
5	DNS	deletes all entries and constructs new entries	deletes all entries and constructs new entries
6	Downloads	◎	◎
7	Searched keywords	◎	◎
8	Typed URLs	◎	◎
9	Visited pages	◎	◎

For Mozilla Firefox and Google Chrome, a single button, Clean History and Close, erases the browser data relating to domestic violence support websites. The interface guarantees that its functionality is both simple and precise. The button not only initiates the cleaning process but also automatically closes the system once completed. To streamline usage and maintain the intended operation, the option to close the system from the taskbar has been removed, forcing users to use this

button. During the cleaning process, feedback is supplied to remind the user to wait until the operation is complete. The overview of the application and processes is illustrated in figure 4.
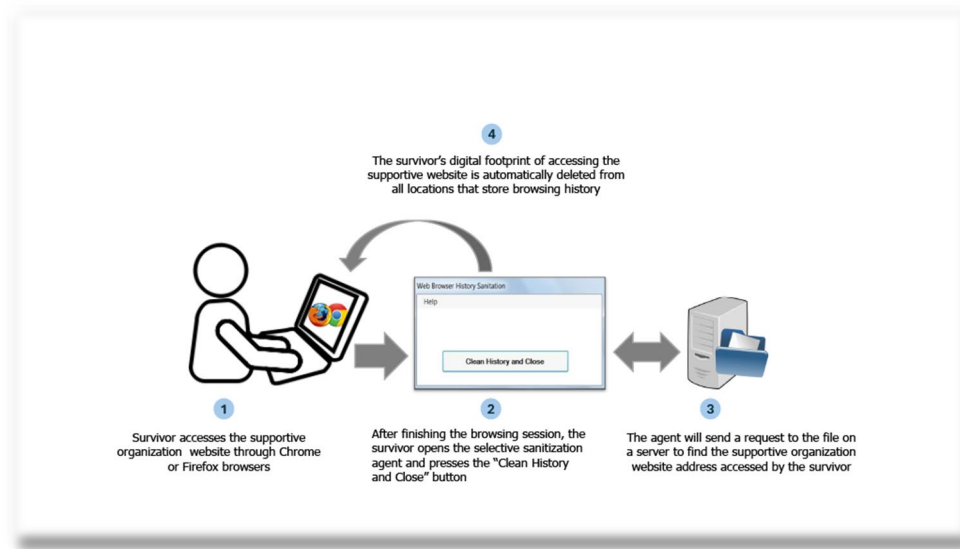

Figure 4: Overview of the application.

4.2. Artifact Evaluation

In the design science framework, artifact evaluation represents the second phase. During this stage, the authors conducted iterative testing cycles to ensure continuous assessment, analyze system behavior, and refine processes. The findings were systematically documented in each cycle to enhance improvement and accuracy.

During the testing phase, the system was tasked with deleting entries related to the domestic violence support website "angelou-centre" (www.angelou-centre.org.uk), which is an actual support organization. We used its address for testing purposes after obtaining their consent. The test consisted of accessing the main website, opening two sub-links, and bookmarking the main page. The history locations were then tracked before and after the system was run, with the results documented in every cycle. In several testing cycles, the authors validated the results and ensured that the system was functioning as planned with accurate results.

The agent automatically downloaded a list of domestic violence support websites (a list of websites stored in a file located on a remote page online). However, the copy of this page was saved locally in case of interruption in connection to the page. In such a situation, the agent used the local copy. As a result, the agent used this file to decide which entries to delete. The list will be updated when new domestic violence support websites go online; likewise, the local file will be updated whenever the system is connected to the remote copy of the file. The consistency of both files contents is assured in this manner.

The analysis of the evaluation phase reveals that the system functions as intended, allowing survivors to access domestic violence support websites using Mozilla Firefox or Google Chrome. After browsing and approaching the desired supportive websites, they simply close the browsers and open the system, which erases any traces of their activity while retaining other data to prevent the abuser's suspicion.

Below is an example demonstrating the system in action with results for the history list. In this scenario, the user opened Mozilla Firefox and accessed the domestic violence support website www.angelou-centre.org.uk. A sub-link from the main page was also visited. Figure 5 displays Firefox's history list, showing records related to www.angelou-centre.org.uk alongside other browsing history.
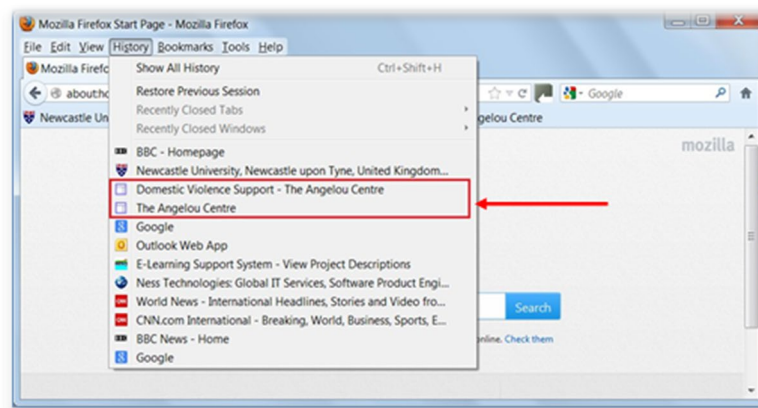
Figure 5: History list entries before running the application.
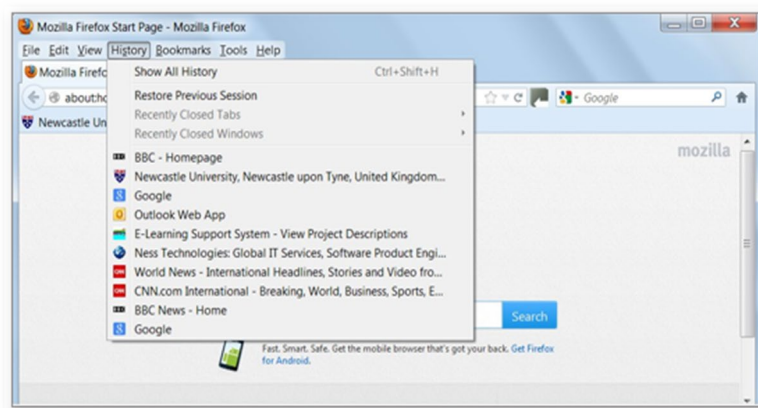
Figure 6: History list entries after running the application.

After running the system, the Mozilla Firefox history list was reviewed. As shown in figure 6, all records related to www.angelou-centre.org.uk were successfully deleted, while all other browsing history remained intact.

The results for other locations, including the cache, cookies, bookmarks, DNS, downloads, searched keywords, visited pages, and typed URLs, are presented in the appendix section.

5.   Discussion

The rising number of domestic violence victims globally underscore the urgent need to implement technological solutions that promote social inclusion for survivors by improving their ability to avoid leaving electronic footprints when they access digital services and seek help online.

In the present day, a number of tools and techniques are available that protect the privacy of users while they are browsing [22, 23, 26, 28, 32, 35]. However, these tools are not specifically designed for domestic violence survivors. Additionally, the majority of these techniques necessitate a certain degree of technical skill to be implemented effectively. The analysis of related work revealed that only Emms *et al* [7] investigated technology-based solutions to assist survivors of domestic violence. Nevertheless, this study has certain limitations, as it has only provided a brief overview of potential approaches and lacked in-depth technical explanations, implementation details, and thorough testing.

By introducing a developed, targeted history sanitization agent—a solution specifically designed to assist domestic violence survivors in safely accessing digital resources—this study has addressed a critical gap. The developed system selectively removes sensitive browsing data related to supportive organizations' websites while preserving other activities and entries to avoid abuser suspicion. This solution emphasizes usability for survivors, in particular for those with no or limited technical expertise.

5.1. Theoretical and Practical Implications

Theoretically, this study extends the body of knowledge on cyberstalking and advances an understanding of how internet technology, notably web browsers, can both help and harm domestic violence survivors. The study aims to provide a multidisciplinary framework for understanding, as well as mitigating, cyber risks for survivors. Additionally, the targeted history sanitization agent developed and presented in this study serves as a foundation for future research into adaptive privacy-preserving technologies that address the specific needs of people who are vulnerable, such as domestic violence survivors, in particular, for those with no or limited technical skills.

The utilization of this solution directly addresses a crucial privacy issue for survivors, allowing them to access support resources while leaving no visible digital footprint that may lead to additional harm by abusers. This study offers actionable insights for organizations that support survivors, promoting the use of privacy-focused tools and procedures to improve the effectiveness of their digital services.

5.2. Limitations and Future Direction

Despite the significant efforts put into this project, there are some limitations of the system, including features that were not implemented due to the scope of the current project.

The principal challenge of this study was the limited implementation of selective cleaning features in all browsers due to time constraints, as at this stage, the authors only considered FireFox and Chrome browsers. The selective deletion of entries in cache and DNS is not implemented in the current system; at this phase, temporary solutions are provided. As mentioned earlier, the cache entries are all deleted, and DNS entries are all deleted and replaced by new random entries to avoid suspicion.

A future study will aim to overcome these constraints by implementing the system for all major and popular other browsers, as well as developing methods for quickly handling binary file formats in order to allow for the accurate management and manipulation of browser cache data to allow for a selectively cleaning feature in addition to DNS entries. The authors aim to develop additional strategies and tools, including browser extensions that allow survivors to selectively delete their search history, ensuring better anonymity of their sensitive queries. For future work, the authors' objective is to consider engaging survivors and privacy experts in the process and accordingly improving the system based on their feedback to ensure that the system is more effective and fits their needs.

6. Conclusions

This article presents a comprehensive exploration of a novel solution aimed at fostering social inclusion for the survivors of domestic violence. The implemented system prioritizes the safety and privacy of survivors seeking online support by allowing them to access online supportive services without leaving behind vulnerable digital footprints. It achieves this by selectively deleting browsing history entries related to support websites, while retaining unrelated entries to minimize the risk of raising the suspicion of abusers.

This study is based on the principles of the design science framework, which was adopted to address the identified problem through the rigorous development and evaluation of the artifact. This approach ensured the creation of a system that is both practical and effective in solving a real-world challenge. The key contribution of this work lies in the development of an innovative artifact that addresses an urgent and existing social challenge, offering a significant step forward in protecting and empowering survivors of domestic violence in the digital age.

References

[1]   B. Olaniran, "ICTs and domestic violence (DV): Exploring intimate partner violence (IPV)," *International Journal of Big Data and Analytics in Healthcare (IJBDAH).*, vol. 6, pp. 31–44, Jan. 2021, doi: 10.4018/IJBDAH.20210701.oa3.

[2]   A. L. Kranz and K. Nakamura, "Helpful or harmful? how innovative communication technology affects survivors of intimate violence," Apr. 2002, [Online]. Available: https://api.semanticscholar.org/CorpusID:148213549.

[3]   A. van Moorsel, M. Emms, G. Rendall, and B. Arief, "Digital strategy for the social inclusion of survivors of domestic violence," 2011. [Online]. Available: https://www.cs.kent.ac.uk/people/staff/ba284/home/Papers/TR1277.pdf.

[4]   B. Arief, K. P. L. Coopamootoo, M. Emms, and A. Van Moorsel, "Sensible privacy: How we can protect domestic violence survivors without facilitating misuse," *Proceedings of the 9th ACM conference on Computer and communications security*, pp. 201–204, 2014, doi: 10.1145/2665943.2665965.

[5]   T. Hand, D. Chung, M. Peters, and A. D. and F. V. C. University of New South Wales, The use of information and communication technologies to coerce and control in domestic violence following separation. Australian Domestic and Family Violence Clearinghouse, 2009.

[6]   C. Southworth, J. Finn, S. Dawson, C. Fraser, and S. Tucker, "Intimate partner violence, technology, and stalking," *Violence Against Women*, vol. 13, no. 8, pp. 842–856, 2007, doi: 10.1177/1077801207302045.

[7]   M. Emms, B. Arief, and A. van Moorsel, "Electronic footprints in the sand: technologies for assisting domestic violence survivors BT - privacy technologies and policy," in *Lecture Notes in Computer Science*, 2014, pp. 203–214.

[8]   D. Canali, L. Bilge, and D. Balzarotti, "On the effectiveness of risk prediction based on users browsing behavior," *Proceedings of the 9th ACM symposium on Information, computer and communications security*, pp. 171–181, 2014, doi: 10.1145/2590296.2590347.

[9]   R. D. P. Daniel and R. P. Sundarraj, "A latent factor model based movie recommender using smartphone browsing history," *Int. Conf. Res. Innov. Inf. Syst. Proceedings of the International Conference on Research and Innovation in Information Systems (ICRIIS).*, pp. 1–6, 2017, doi: 10.1109/ICRIIS.2017.8002510.

[10]   P. Shuxin *et al.*, "A method of behavior evaluation based on web browsing information," *Proceedings - 2017 International Conference on Smart Grid and Electrical Automation (ICSGEA 2017).*, , pp. 697–700, 2017, doi: 10.1109/ICSGEA.2017.70.

[11]   A. Dabrowski, G. Merzdovnik, N. Kommenda, and E. Weippl, "Browser history stealing with captive Wi-Fi portals," *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops (SPW 2016).*, pp. 234–240, 2016, doi: 10.1109/SPW.2016.42.

[12]   K. Sim, H. Heo, and H. Cho, "Combating web tracking: analyzing web tracking technologies for user privacy," *Future Internet*, vol. 16, no. 10, 2024, doi: 10.3390/fi16100363.

[13]   A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, Dec. 2004, doi: 10.2307/25148625.

[14]   S. T. March and V. C. Storey, "Design science in the information systems discipline: an introduction to the special issue on design science research," *MISQuarterly* , vol. 32, no. 4, pp. 725–730, Dec. 2008, doi: 10.2307/25148869.

[15]   S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact," *MISQuarterly* , vol. 37, no. 2, pp. 337–355, Dec. 2013, [Online]. Available: http://www.jstor.org/stable/43825912.

[16]   K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, [Online]. Available: http://www.jstor.org/stable/40398896.

[17]   F. Stevens, J. R. C. Nurse, and B. Arief, "Cyber Stalking, cyber harassment, and adult mental health: a systematic review," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 6, pp. 367–376, Nov. 2020, doi: 10.1089/cyber.2020.0253.

[18]   U.S. Department of Justice, "OVW observes national stalking awareness month, 2023," *Office on Violence Against Women*, 2023. https://www.justice.gov/ovw/blog/ovw-observes-national-stalking-awareness-month-2023 (accessed Nov. 14, 2024).

[19]   Kaspersky, "Global Kaspersky report reveals digital violence has increased," *Kaspersky*, 2024. https://www.kaspersky.com/about/press-releases/global-kaspersky-report-reveals-digital-violence-has-increased (accessed Oct. 15, 2024).

[20]   Office for National Statistics, "I feel like I am living someone else's life': one in seven people a victim of stalking," *UK Office for National Statistics*, 2024. https://shorturl.at/HUnOW (accessed Nov. 23, 2024).

[21]   M. Sheridan, "The latest cyberstalking statistics for 2024," *SafeHome.Org*, 2024. https://www.safehome.org/data/cyberstalking-statistics/ (accessed Nov. 01, 2024).

[22]   K. Hughes, P. Papadopoulos, N. Pitropakis, A. Smales, J. Ahmad, and W. Buchanan, "Browsers' private mode: is it what we were promised?," *Computers*, vol. 10, Dec. 2021, doi: 10.3390/computers10120165.

[23]   R. Shah, P. Shukla, D. Rathod, S. Hitesh, and Y. Zala, "Web browser forensics: mozilla firefox," *International Journal of*

Electronic Security and Digital Forensics, vol. 1, p. 1, Jan. 2024, doi: 10.1504/IJESDF.2024.10055704.

[24] D. Mugisha, "Web browser forensics: Evidence collection and analysis for most popular web browsers usage in windows 10," *International Journal of Cyber Criminology*, vol. 54, p. 12, Sep. 2018, doi: 10.13140/RG.2.2.25857.51049.

[25] P. Anuradha, T. R. Kumar, and N. V. Sobhana, "Recovering deleted browsing artifacts from web browser log files in Linux environment," *2016 Symposium on Colossal Data Analysis and Networking (CDAN 2016)*, pp. 1–4, 2016, doi: 10.1109/CDAN.2016.7570957.

[26] O. R. Hammoud and I. A. Tarkhanov, "A method to prevent tracking browsing history with the use of browser extension," *UBMK 2019 - Proceedings of 4th International Conference on Computer Science and Engineering*, pp. 251–254, 2019, doi: 10.1109/UBMK.2019.8907084.

[27] I. Sanchez-Rola, D. Balzarotti, and I. Santos, "Cookies from the past: timing server-side request processing code for history sniffing," *Digital Threats: Research and Practice*, vol. 1, no. 4, 2020, doi: 10.1145/3419473.

[28] J. Bou Abdo and S. Zeadally, "Disposable identities: Solving web tracking," *Journal of Information Security and Applications*, vol. 84, no. June, p. 103821, 2024, doi: 10.1016/j.jisa.2024.103821.

[29] L. Olejnik, C. Castelluccia, and A. Janc, "On the uniqueness of Web browsing history patterns," *Annales des Telecommunications/Annals of Telecommunications*, vol. 69, no. 1–2, pp. 63–74, 2014, doi: 10.1007/s12243-013-0392-5.

[30] A. Aggarwal, B. Viswanath, L. Zhang, S. Kumar, A. Shah, and P. Kumaraguru, "I spy with my little eye: analysis and detection of spying browser extensions," *P Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018*, no. Section 3, pp. 47–61, 2018, doi: 10.1109/EuroSP.2018.00012.

[31] Z. Wang, F. X. Lin, L. Zhong, and M. Chishtie, "How effective is mobile browser cache?," *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, pp. 17–19, 2011, doi: 10.1145/2030686.2030693.

[32] Y. Wu, D. Meng, and H. Chen, "Evaluating private modes in desktop and mobile browsers and their resistance to fingerprinting," *Proceedings of the 2017 IEEE Conference on Communications and Network Security, CNS 2017*, vol. 2017-Janua, pp. 1–9, 2017, doi: 10.1109/CNS.2017.8228636.

[33] Y. Wu, P. Gupta, M. Wei, Y. Acar, S. Fahl, and B. Ur, "Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode," *Proceedings of the World Wide Web Conference (WWW 2018)* , pp. 217–226, 2018, doi: 10.1145/3178876.3186088.

[34] A. Shoeb, "Is private browsing in modern web browsers really private?," Jan. 2018, doi: 10.48550/arXiv.1802.10523.

[35] A. Kumar *et al.*, "Forensics analysis of TOR browser," in *Lecture Notes in Electrical Engineering*, 2024, vol. 1075 LNEE, pp. 331–341, doi: 10.1007/978-981-99-5091-1_24.

[36] W. L. Chen and W. G. Teng, "Exploiting browsing history for exploratory search," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5617 LNCS, no. PART 1, pp. 355–364, 2009, doi: 10.1007/978-3-642-02556-3_41.

[37] A. van der Merwe, A. Gerber, and H. Smuts, "Guidelines for conducting design science research in information systems," *Communications in Computer and Information Science*, Jul. 2019, vol. 1136 CCIS, pp. 163–178, doi: 10.1007/978-3-030-35629-3_11.

[38] A. Ahmed, S. Ahmad, N. Ehsan, E. Mirza, and S. Z. Sarwar, "Agile software development: Impact on productivity and quality," *5th IEEE International Conference on Management of Innovation and Technology (ICMIT2010)* , pp. 287–291, 2010, doi: 10.1109/ICMIT.2010.5492703.

[39] M. Stoica, M. Mircea, and B. Ghilic-Micu, "Software development: Agile vs. traditional," *Informatica Economică.*, vol. 17, no. 4, 2013, doi: 10.12948/issn14531305/17.4.2013.06.

[40] M. B. Legowo, B. Indiarto, and D. Prayitno, "Agile software methodology with scrum for developing quality assurance system," *Proceedings of the 2nd International Conference of Computer and Informatics Engineering: Artificial Intelligence Roles in Industrial Revolution 4.0, IC2IE 2019* , pp. 104–109, Sep. 2019, doi: 10.1109/IC2IE47452.2019.8940831.

Appendix

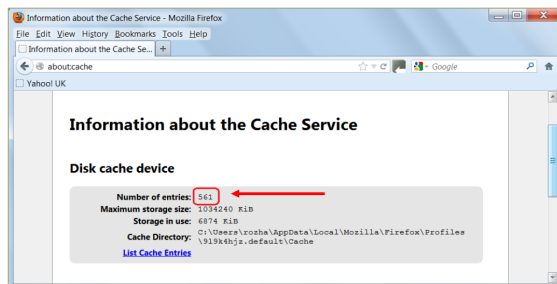### A. *Cache entries before and after running the application*

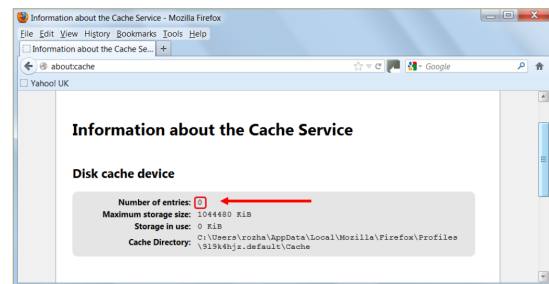**Figure 7**: Cache entries before running the application.

Figure 8: Cache entries after running the application.

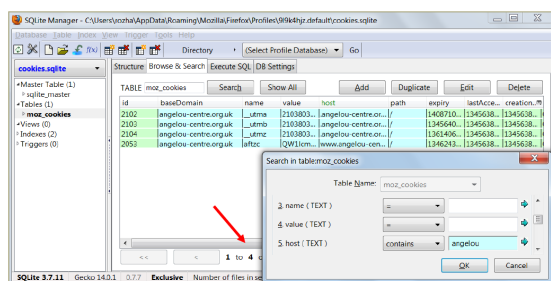### B. *Cookies entries before and after running the application*

Figure 9: Cookies entries before running the application - searching for Angelou records.
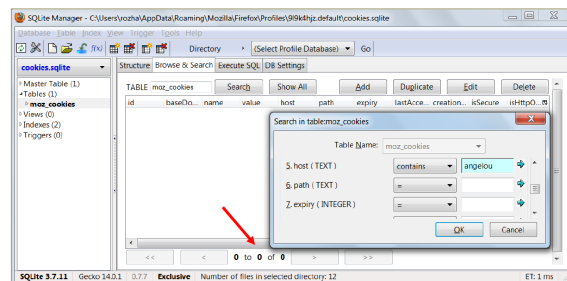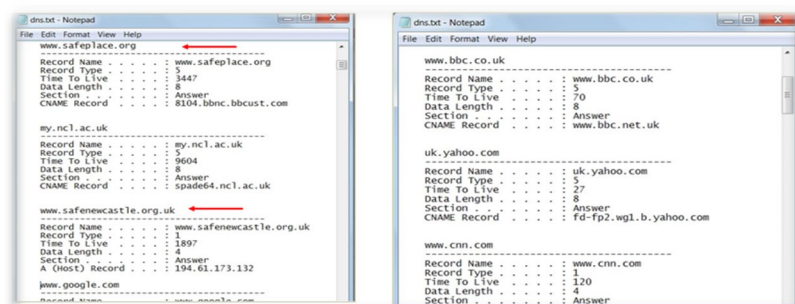
Figure 10: Cookies entries after running the application - searching for Angelou records.

C. *Bookmarks entries before and after running the application*
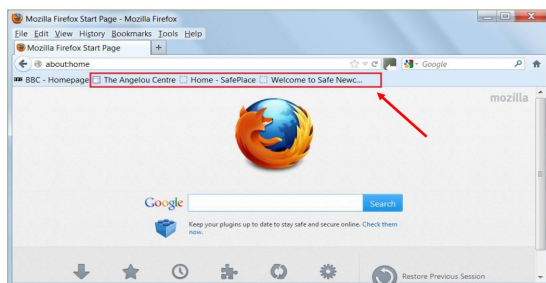
Figure 11: Bookmarks entries before running the application.

Figure 12: Bookmarks entries after running the application.

D. *DNS entries before and after running the application*

Figure 13: DNS entries before and after running the application.

E. *Download entries before and after running the application*

Figure 14: Download entries before running the application.

Figure 15: Download entries after running the application.

F. *Searched keyword entries before and after running the application*

Figure 16: Searched keywords before running the application - searching for the Angelou center.

Figure 17: Searched keywords after running the application - searching for the Angelou center.

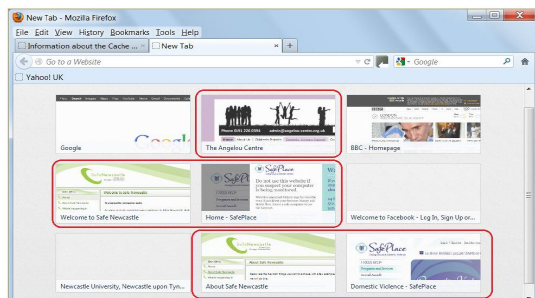## G. *Visited page entries before and after running the application*

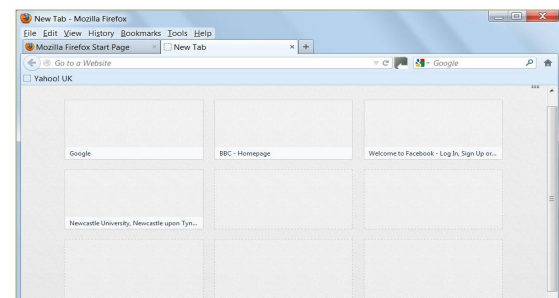**Figure 18**: Visited pages before running the application.

Figure 19: Visited pages after running the application.

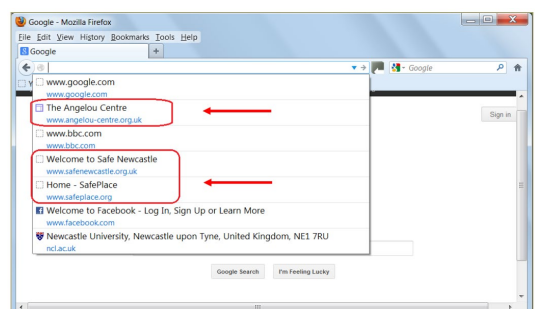## H. *Typed URLs before and after running the application*

Figure 20: Typed URLs before running the application – searching for the Angelou center URL
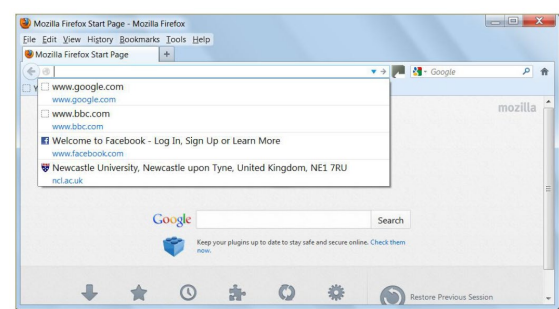

Figure 21: Typed URLs after running the application – searching for the Angelou center URL