Report

**INT301: Open Source Technologies**

Continuous Assessment

By

Gagandeep Pandit

11903663

Roll no: 16



School Of Computer Science and Engineering

Lovely Professional University, Punjab

**Introduction**

* 1. **Objective of the project**

The objective of this project is to capture and analyze the browser history using open source tools. The project aims to perform a thorough scan of the user's bookmarks, cache data, visited websites, and cookies to gather as much information as possible. The tool will be designed to work with popular web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge. The project aims to provide a useful tool for security experts, forensic investigators, and other professionals who need to analyze browser history data.

**1.2 Description of the project**

The project involved using the Autopsy tool to analyze the browser history of a target system. Autopsy is an open-source digital forensic tool that provides a graphical interface to analyze data on a system. The tool was used to extract the browser history data, including bookmarks, cache data, visited websites, and cookies.

Here are the steps to use Autopsy to capture browser history:

1. Install Autopsy: The first step is to download and install Autopsy from the official website.
2. Create a new case: Once Autopsy is installed, launch the application and create a new case. Give the case a name and location to store the case file.Graphical user interface, text, application, email

   Description automatically generated
3. Add image: To add the image of the device you want to analyze, click on the "Add Data Source" button and select "logical file." Browse to the location of the file and add it to the case.

Graphical user interface, application

Description automatically generated

1. Add module: After adding the image file, click on the "Add Module" button and select "Web Browser History." This will add the module for extracting browser history.

Graphical user interface, application

Description automatically generated

1. Configure module: Once the module is added, configure it by selecting the browser you want to extract history from. Autopsy supports various web browsers, including Chrome, Firefox, Safari, and Internet Explorer.
2. Run the analysis: After configuring the module, click on the "Run" button to start the analysis. Autopsy will scan the image file and extract the browser history.
3. View results: Once the analysis is complete, you can view the extracted browser history by clicking on the "Browser History" tab. You can filter the results by date, URL, title, and other criteria.

Export results: If you need to export the browser history, you can do so by clicking on the "Export" button and selecting the format you want to export the results in.

**1.3 Scope of the project**

The scope of this project includes capturing and analyzing web browsing history from a target system using Autopsy. The project focuses on identifying the following web browsing history artifacts:

Bookmarks: URLs that have been bookmarked by the user.

Cache data: Information that has been stored in the cache, such as images and scripts.

Visited websites: URLs that have been visited by the user.

Cookies: Information that has been stored in cookies, such as login credentials and session IDs.

**System Description**

**2.1 Target system description**

Edition-Windows 11 Home Single Language

Installed RAM-16.0 GB (15.8 GB usable)

Storage – 237 GB (C:\) 931 GB (D:\)

System type-64-bit operating system, x64-based processor

**2.2 Assumptions and Dependencies**

The project assumed that the user had not deleted the browsing history and that the Autopsy tool would be able to extract the data successfully. The project also depended on the availability of the target system and the Autopsy tool.

**2.3 Functional/Non-Functional Dependencies**

The functional dependencies of the project included the ability of Autopsy to extract the browser history data successfully. The non-functional dependencies included the performance of the system and the availability of storage space for the extracted data.

**2.4 Data set used**

The data set used in support of the project was the browser history data extracted from the target system using Autopsy. The data set included the bookmarks, cache data, visited websites, and cookies for the all the browsers on the system like Google Chrome, Firefox, Brave, etc.

**Project Screenshots (GITHUB REPO LINK -** [**https://github.com/Gagandeep-Pandit/INT301-PROJECT**](https://github.com/Gagandeep-Pandit/INT301-PROJECT) **)**

Captured Browser Data:Graphical user interface, text, application

Description automatically generated

Bookmarks:

Text

Description automatically generated

Cache Data:

Graphical user interface

Description automatically generated

Cookies:

Graphical user interface, application, table

Description automatically generated

Visited Websites:

Graphical user interface, application

Description automatically generated

**References**

* Carrier, B. (2014). File System Forensic Analysis. Upper Saddle River, NJ: Addison-Wesley.
* Casey, E., & Stellatos, G. (2014). Digital Forensics with Open Source Tools. San Francisco, CA: Elsevier.
* Cohen, F. (2011). The Google Hacker's Guide. Burlington, MA: Syngress.
* Garfinkel, S., & Shelat, A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practices. Digital Forensic Research Workshop.
* Garfinkel, S. (2010). Digital Forensics Research: The Next 10 Years. Digital Investigation, 7(S1), S64-S73.
* Rouse, M. (2015). Autopsy Forensic Browser. Retrieved from <https://searchsecurity.techtarget.com/definition/Autopsy-forensic-browser>
* The Sleuth Kit (TSK) & Autopsy. (n.d.). Retrieved from

<https://www.sleuthkit.org/autopsy/>

* Wu, X., Zhang, J., & Wang, G. (2015). A Survey of Web Browser Forensics. Digital Investigation, 14, 69-83.
* These references provide information on digital forensics, file system analysis, web browser forensics, and the Autopsy tool.