Open Source Technologies (INT-301)

CA-3 (Project)

Question no. - 29

Name - Manoj Kumar

Roll no. – 16

Reg. no. – 11906058

1. Introduction :-
   1. Objective of Project –

Capture and analyse the browser history using any open source tool. Perform a scan of bookmarks and visited websites.

* 1. Description of the project –

Browser forensics is the process of analyzing digital artifacts left behind by a user's web browsing activity. This includes information about the websites they have visited, their browsing history, and their bookmarks.

To capture this information, forensic analysts typically use specialized software tools that are designed to extract data from a user's browser cache, cookies, history, and bookmarks files.

The browsing history contains a list of websites that the user has visited, including the date and time of each visit. This can provide valuable information about the user's online activity, such as their interests, habits, and behavior.

Bookmarks are shortcuts to specific websites that the user has saved for easy access. They can provide insight into the user's favorite websites, as well as their priorities and interests.

In addition to browsing history and bookmarks, forensic analysts may also examine cookies, which are small files stored on a user's computer by websites they visit. Cookies can contain information such as login credentials, website preferences, and tracking data, which can be used to track the user's online activity across different websites.

Overall, browser forensics can provide valuable insights into a user's online behavior and activity. However, it is important to note that privacy concerns may arise when collecting and analyzing this information, and appropriate legal and ethical considerations should be taken into account.

* 1. Scope of the Project –

The scope of a browser forensic project can vary depending on the specific goals and objectives of the investigation. However, in general, the scope of a browser forensic project would typically involve the following:

Identification of the browser: The first step in any browser forensic investigation is to identify the browser software used by the user. This may include popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, or Safari.

Acquisition of browser data: Once the browser has been identified, the next step is to acquire the relevant data for analysis. This may include data such as browsing history, bookmarks, cookies, cached files, and download history.

Analysis of browser data: The acquired data is then analyzed to extract relevant information and artifacts that may be useful in the investigation. This may include information such as website URLs, search terms, timestamps, and user account information.

Interpretation of findings: The final step is to interpret the findings and draw conclusions based on the information gathered. This may involve correlating browser data with other digital artifacts or physical evidence, as well as using specialized tools and techniques to analyze the data.

1. System Description :-

Device name LAPTOP-LLTBOQAN

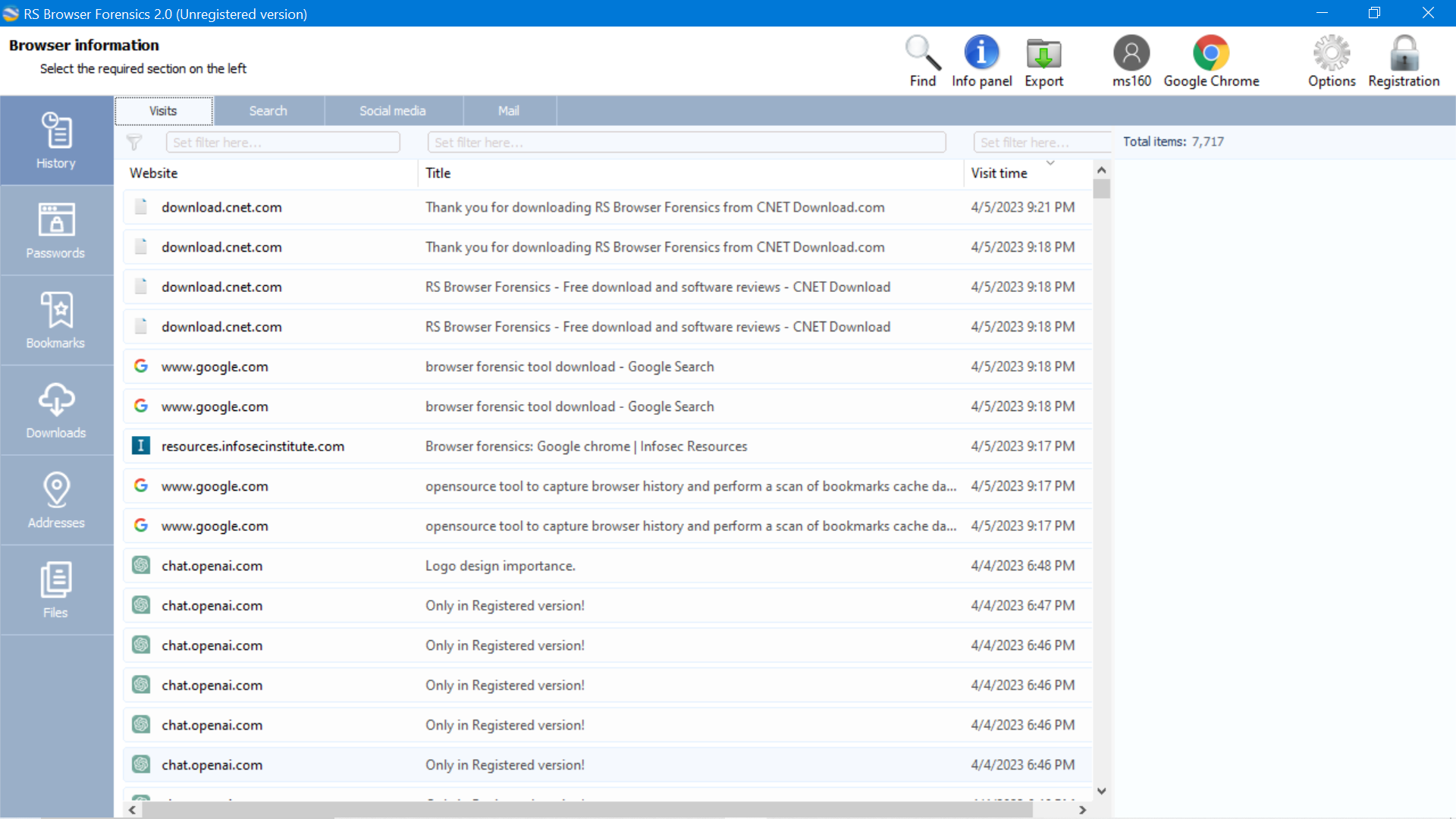
Processor Intel(R) Core(TM) i3-8145U CPU @ 2.10GHz 2.30 GHz

Installed RAM 4.00 GB (3.86 GB usable)

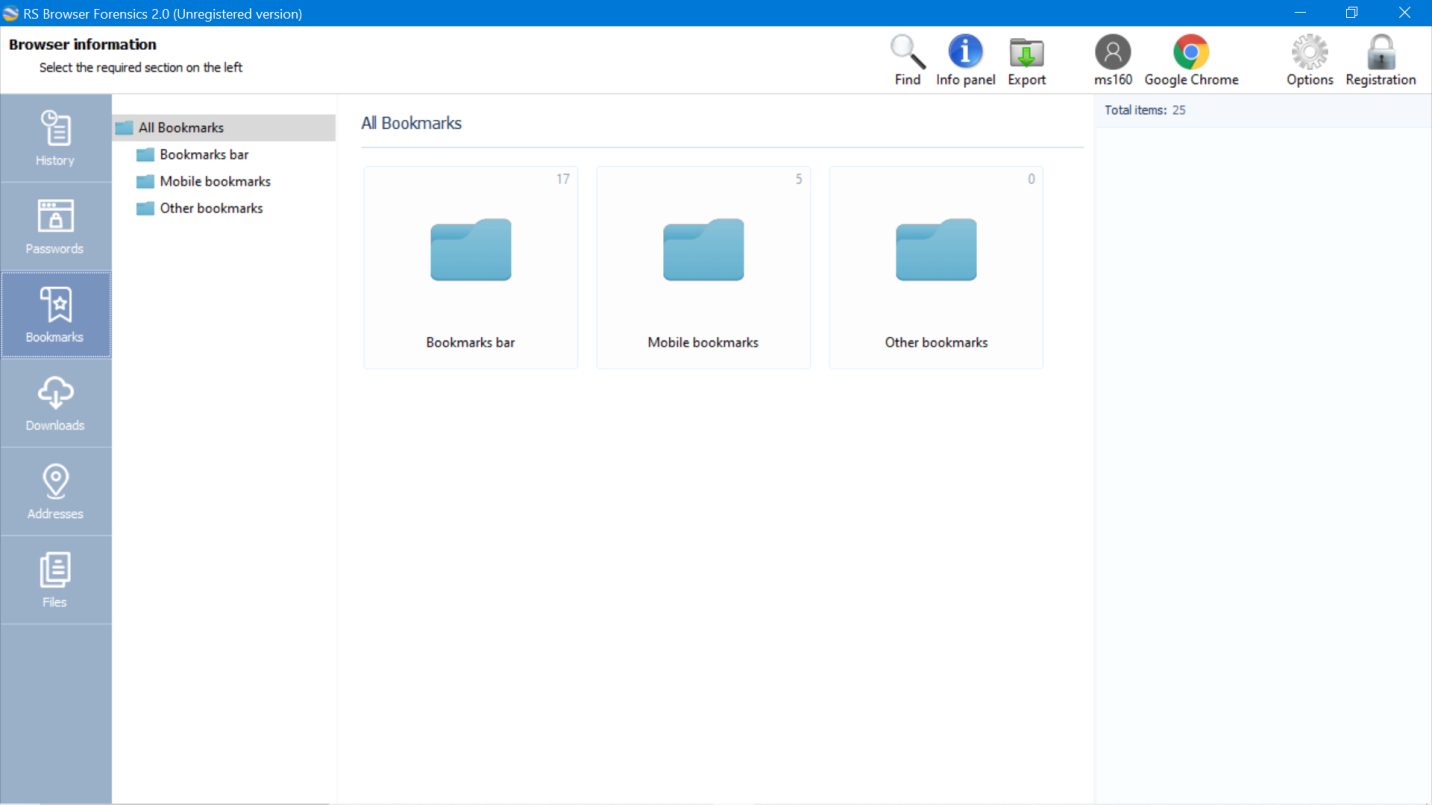
System type 64-bit operating system, x64-based processor

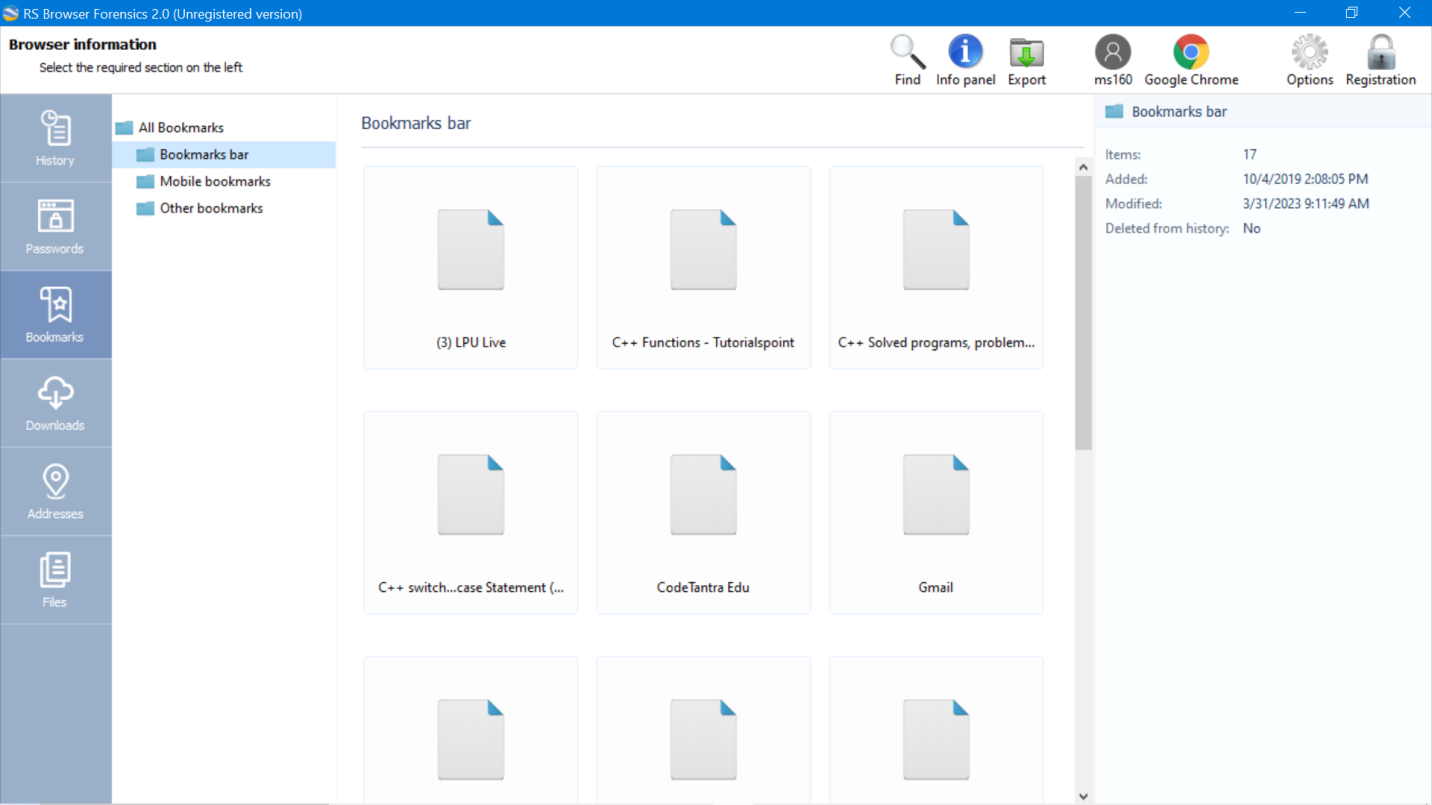
1. Analysis report :-

Browser history snapshot –

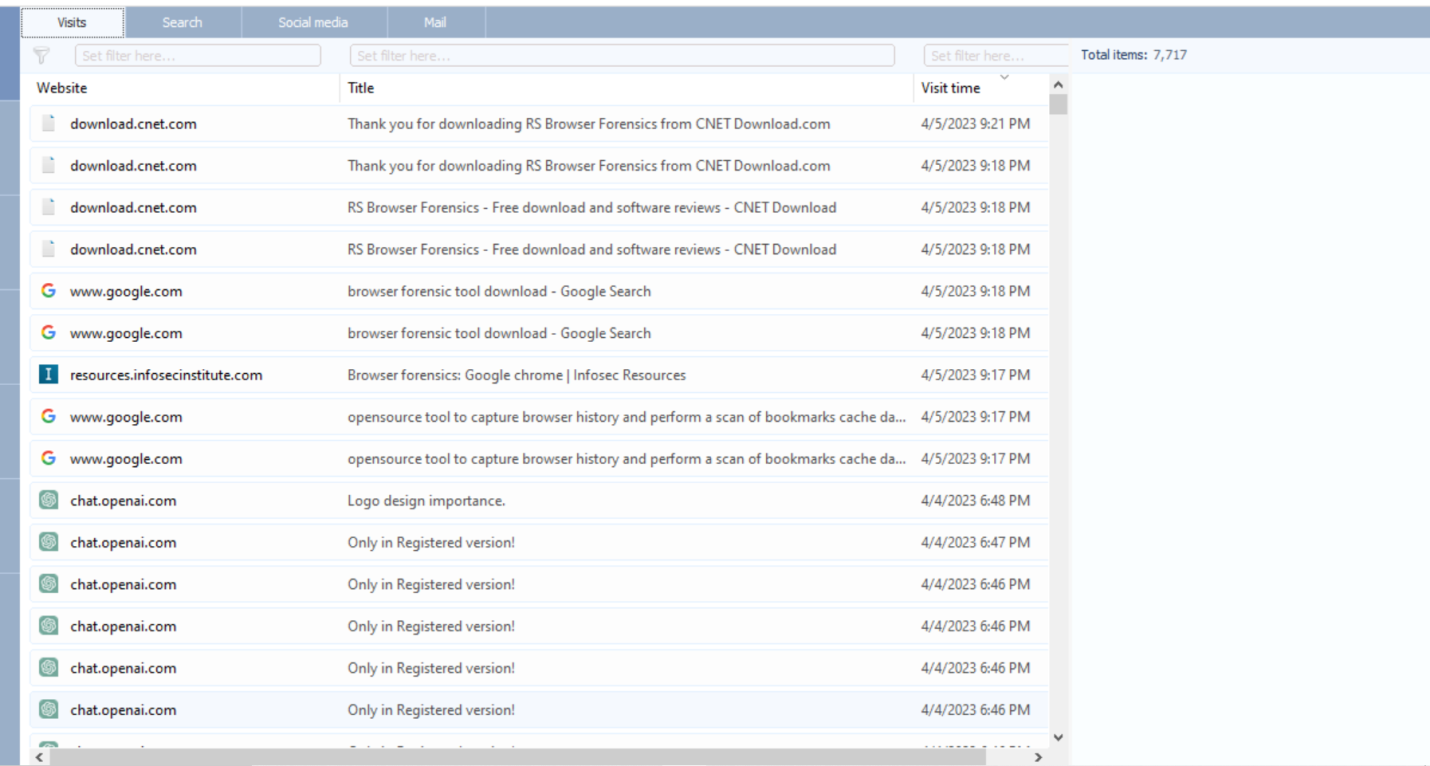


Bookmarks snapshots –





Visited websites snapshot :-



Files :-

