Scratch and Script Ltd

Digital Forensics Lab Creation Series.

Dear students, you are expected to develop various labs in Digital Forensics every week for your skill enhancement and portfolio building. You shall be submitting on the google classroom for evaluation and review:

NB:/ The lab you shall come up with should include screenshots of the actual expected activities i.e., you will practically have to do the lab.

Web Activity Forensics:
Develop a lab activity that focuses on Web activity forensics and as you can imagine already, web activity is done via a web browser. The recommended browser is ***Google Chrome***.

Guidelines:

1. The relevant data can be found on this path:
   C:\Users\[USERNAME]\AppData\Local\Google\Chrome\UserData\Default.

2. The files have different file formats, but often SQLLite is used.
   Links to SQLite browsers that you can use:
   DB Browser for SQLite (DB4S): https://sqlitebrowser.org/

   SQLite project provides a simple command-line program named sqlite3 (or sqlite3.exe on Windows) that allows the user to manually enter and execute SQL statements against an SQLite database or a ZIP archive: https://sqlite.org/cli.html

3. There are various files and folders. The interesting content can be found in the following files:

Content	**Location**	**Format**
List of all visited websites	History	SQLite
Search Words	History	SQLite
A downloaded object of web pages, cached files.	Downloads, Cache	Binary format
Sites Saved	Bookmarks	JSON

Locally stored cookies.	Cookies	SQLite
Most visited websites as these appear on the home page.	TopSites	SQLite
User information used to log into websites.	Login Data	SQLite

4. Locate your copy of the Chrome folder and copy the following files and a folder to some newly created folder:
    - History - take a keen interest in things like *url, visit_count, last_visit, and time, search keywords*
    - Cookies - take a keen interest in things like *host_key path name created expires value*
    - Login Data - you can look at *Short name and Search URL*
    - Web Data

    Cache - Download and install the Chrome Cache View tool
    http://www.nirsoft.net/utils/chrome_cache_view.html
    This involves finding various file types: you can look for image files, video files, web pages

5. Automating using Python: All the previous activities can be automated. It is possible to write simple Python scripts that can extract the required artifacts. See for instance: https://github.com/PacktPublishing/Mastering-Python-for-Networking-and-Security/blob/master/chapter12/ChromeDownloads.py

    (You can select one of the previous types of artifacts and write a simple script to automatically extract them.)

All the best and good luck!