|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2020/21) Semester 4/6 | Week 9 |
| Practical 9 |
| **Familiarization with SQLite** | |

**OBJECTIVES**

1. To be able to make use of a SQLite explorer tool to view database files.

**Overview**

As Windows 10 OS stores artifacts related to Google Chrome, Mozilla Firefox, Skype etc. in database format, we need to use a SQLite explorer tool to view the artifacts extracted from an evidence file. In this practical activity, we will make use of the Acquire Forensic’s SQLite Forensic Explorer to view database files.

Note that Laura.E01 was acquired from a Windows 7 OS computer, hence you need to copy a database file from your own laptop (running Windows 10 OS) for this practical. You may choose from any of these database files, if available:

Google Chrome

Bookmarks, History, Cookies are located in:

C:\Users \%UserName%\ AppData\Local\Google\Chrome\User Data\Default\

Mozilla Firefox

Bookmarks, History are located in:

C:\Users \%UserName%\AppData\Roaming\mozilla\Firefox\ Profiles\xx.default\places.sqlite

Cookies are located in:

C:\Users \%UserName%\AppData\Roaming\mozilla\Firefox\ Profiles\xx.default\cookies.sqlite

Skype

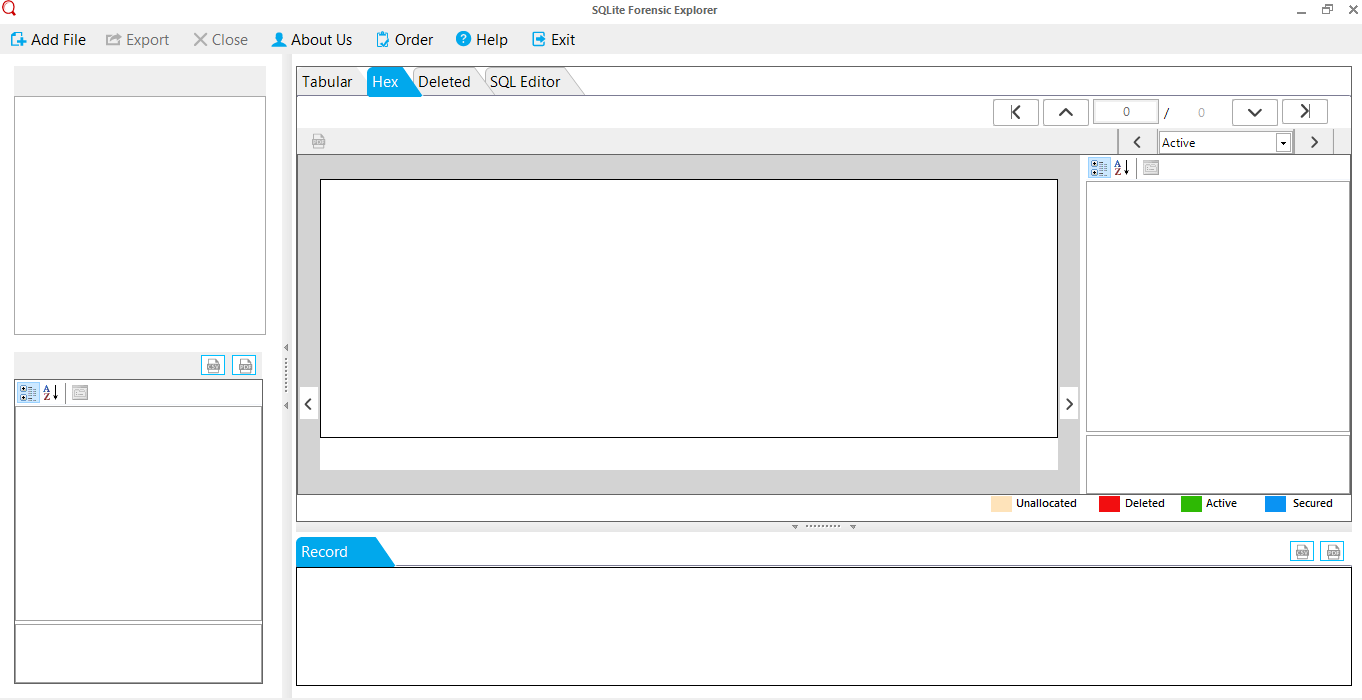
Skype client store the instant messaging history in:

C:\Users\%UserName%\AppData\Roaming\Skype\<aliases>\main.db

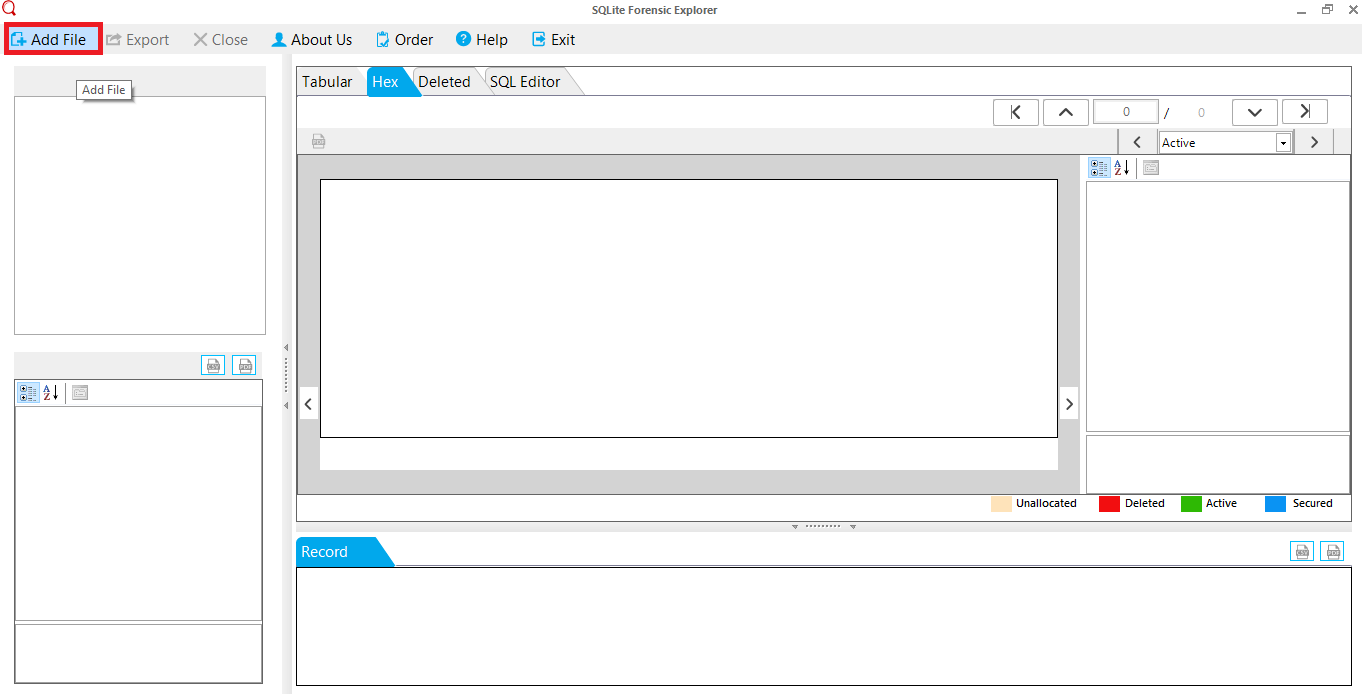
This is just an activity to introduce you to the tool, to prepare you for coming assignment.

Steps:

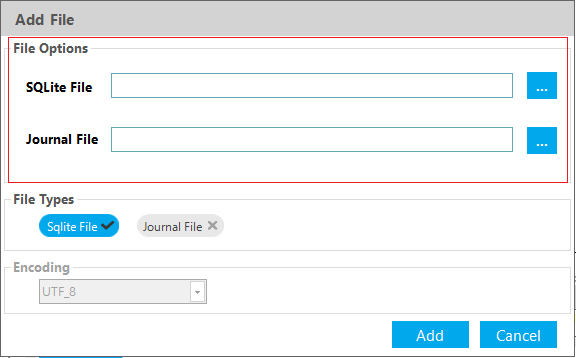
1. Launch SQLite Forensic Explorer from the installed location. To open the software, Go to Start > All Programs > Sqlite Forensic Explorer.



1. Now, click on Add File button on menu bar of the software to add and start the analysis process of the Sqlite file.

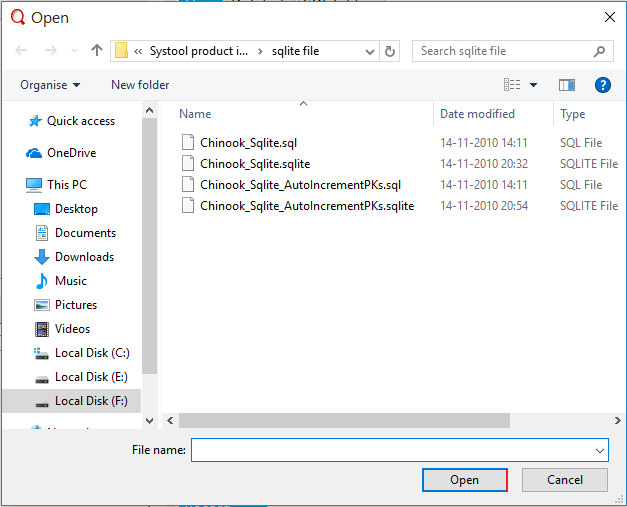


1. A pop-up window will prompt user to Browse and select the file type: either Sqlite File or Journal File.

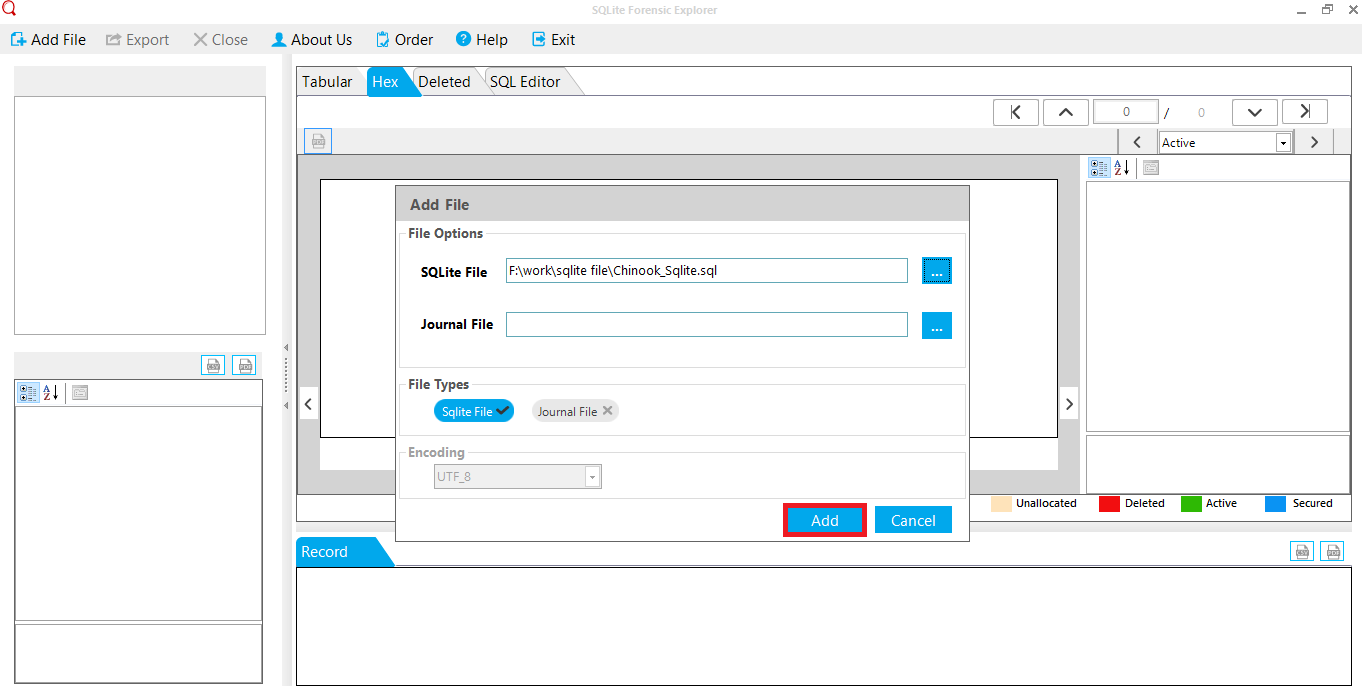


**Note: Your view may be different from the screenshots below as you are using different database files.**

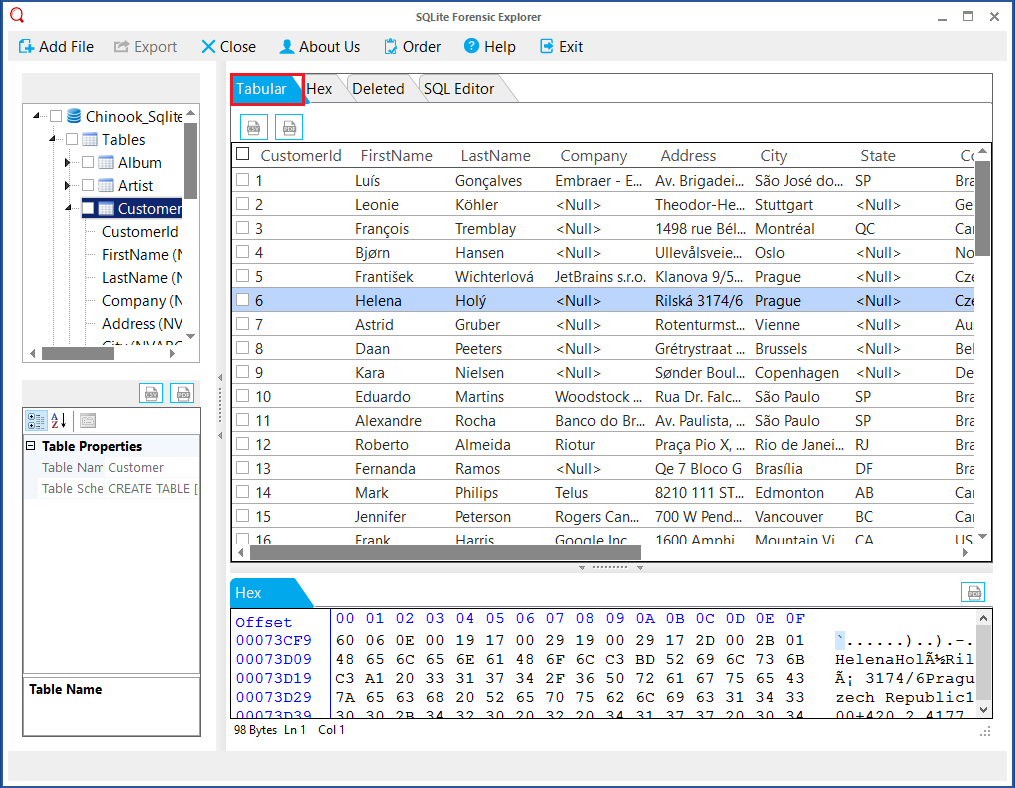
1. Now, click on Browse button to find and open the required Sqlite file from system.



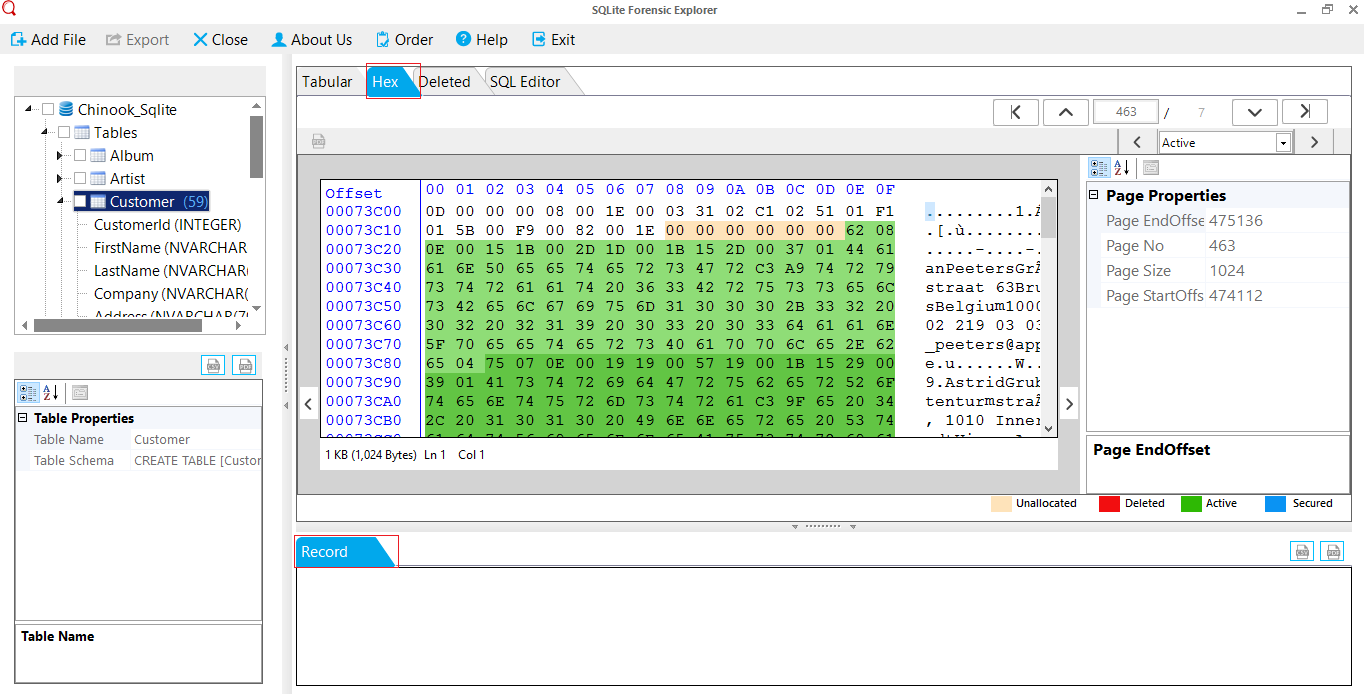
1. Click on Add button on the left panel to start the scanning process of Sqlite file.



1. Now, in next pop-up window left panel shows the tree structure of the folder and right panel under the **Tabular** bar shows the preview of Sqlite file.



1. **Hex tab** in the software assists the user to analyze the email messages in binary format. The **Record** bar shows the complete report of the message.



1. You are encouraged to explore more on the tool on your own.

Reference

* https://www.acquireforensics.com/products/sqlite-forensic-explorer/guide.html

- The End -