

## FQLITE GUIDED EXERCISE

FQLite is a forensic SQL browser offering data recovery and WAL file analysis features. Video walkthrough available on the Tool Walkthrough Playlist at <https://youtube.com/@hexordia>

Prior to going through this process, ensure that the Java Runtime Environment (JRE) is installed. FQLite requires a JRE of version 1.8 or above. The latest JRE may be downloaded from the following link: <https://www.java.com/en/download/manual.jsp>

To get started, please download FQLite from <https://www.staff.hs-mittweida.de/~pawlaszc/fqlite/>

Prior to installation, verify the hash value to the known good from the syllabus for students enrolled in the HMFA Virtual Live course. The SHA1 hash value for the fqlite\_v1.5.8.jar is 554A6D3A0D1BBF0F0745D7C745CFF756.

\*\*If you already have FQLite downloaded, please move on to [Set Up and Use](#).

### INSTALLATION

Once on the installation website, navigate to the latest release and download the associated jar file. A SHA1 hash value of the file can be found underneath each package.

### Download latest version

---

*Jan 17th, 2022*

[Download fqlite\\_v1.5.8.jar](#)

sha1 sum 554a6d3a0d1bbf0f0745d7c745cff756

What's new:

- added support for ROWIDs even for removed records
- replaced hex-editor with a faster version
- sorting of date-columns now works as expected
- wrong sorting of integer-columns is fixed
- fixed issue with last page in free page list

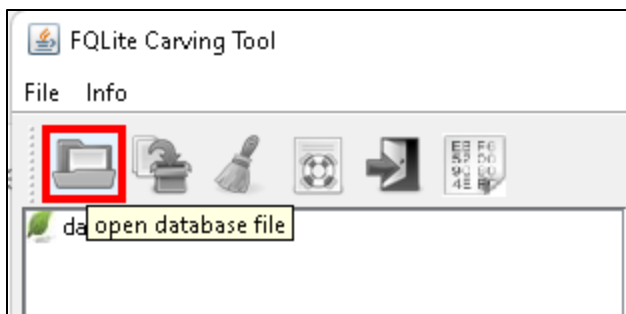
*Jan 4th, 2022 (New Year Edition)*

Once downloaded, if Java is properly installed, FQLite may be ran by clicking on the downloaded jar file.

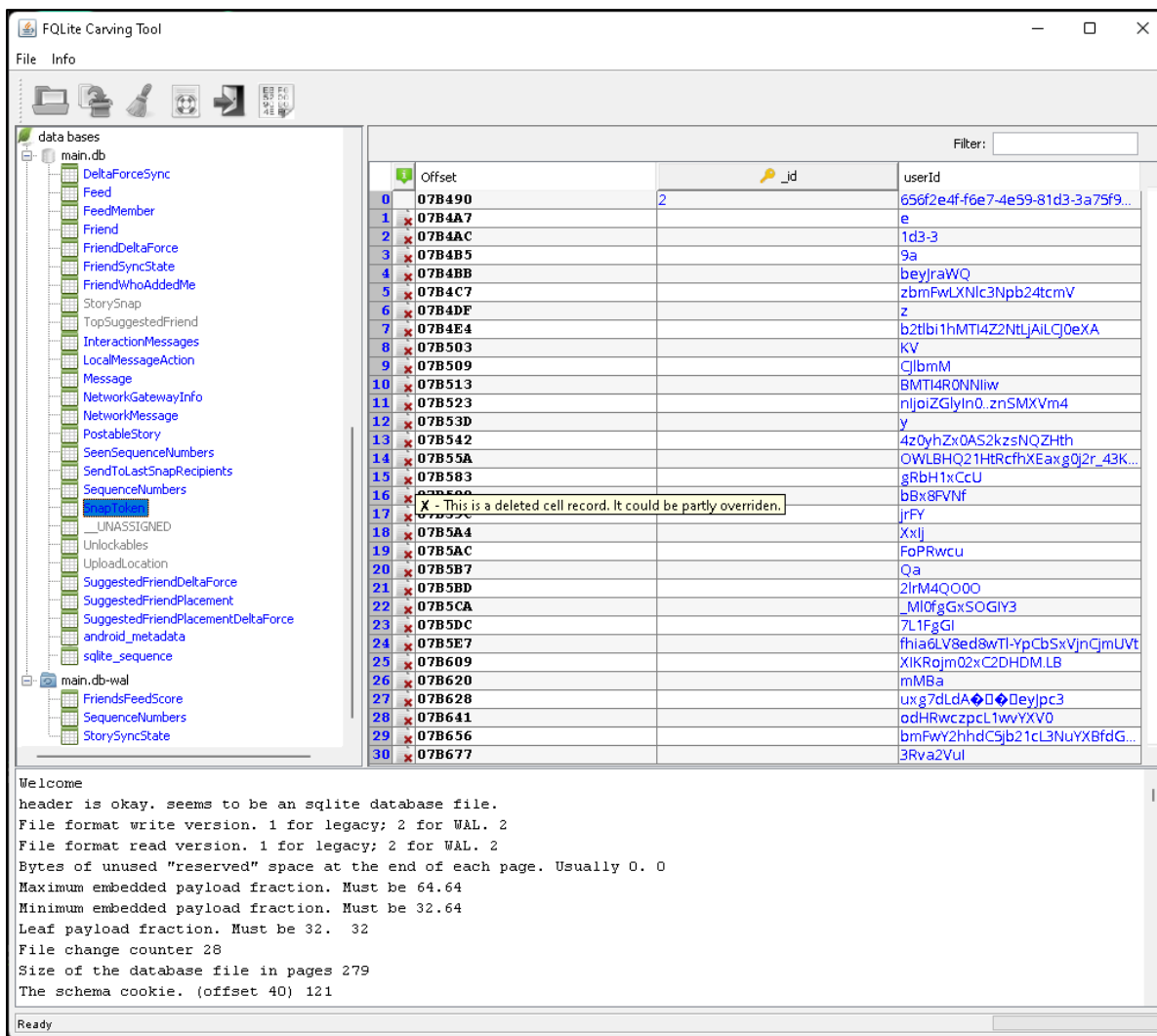
 fqlite_v1.5.8.jar	2/16/2023 11:11 AM	Executable Jar File	8,624 KB
---	--------------------	---------------------	----------

## SET UP AND USE

Open a SQLite database by clicking on the open file icon or by heading to “File” and then “Open database”. Alternatively, databases may be dragged and dropped onto the databases window.



Note that opening a database for the first time in FQLite may present a software bug in which contents of the table are presented as empty when they are actually populated. To best avoid this issue, compare contents of the table found within FQLite with contents of the table viewed in another SQL browser such as DB Browser for SQLite: <https://sqlitebrowser.org/>



After opening a database, if an associated WAL file is found in the same directory the WAL is opened separately. The WAL may be examined separately without applying changes to the main database. Double-clicking on opened databases will present a list of tables held within the database.

Tables which are populated with data appear as blue text next to a database icon. Tables which are empty appear as gray text next to this icon.



The primary key of each table is identified by a key icon next to the column name.



FQLite will attempt to recover deleted entries. When deleted entries are found they are presented within their original tables next to an icon of a document with a red 'x'.



	Offset	_id	userId
0	<b>07B490</b>	2	656f2e4f-f6e7-4e59-81d3-3a75f9...
1	<b>07B4A7</b>		e

