**Processing SQLite Databases using Templates**
**(applicable to forensic analysis and data recovery)**

This article covers the processing of SQLite database files for forensic analysis, security auditing and data recovery purposes. A growing number of software applications on computer systems and mobile devices are using SQLite database to store data. A few examples of usage of SQLite databases includes but is not limited to:

- Software settings, SQLite databases are used to store not only general settings for software applications but you will also find user specific settings.

- Chat history, a number of products use SQLite databases for storing conversations between users on computer and mobile devices.

- Keyloggers, some key logging software use SQLite databases to store all recorded information and is well suited being capable of writing and holding millions of records containing pictures and text information.

- Virtually and data can be stored in a SQLite database…

SQLite databases typically consist of a single (sometimes multiple files linked) with each database file containing one or many tables. Each database table will contain a certain number of columns in a set order and each row or record will store data accordingly. SQLite databases can store virtually any data including:

- Text – this could be human readable or encoded
- Date and Times – any date format or specification of designers choosing
- Binary (BLOB) – this can be pictures, documents or any data of designers choosing.

## Problems and Issues

- Due to the growing number of SQLite databases present in both computer and mobile devices the time to open, process and review the data contained within each SQLite database is becoming problematic.

- Formats change, from time to time SQLite databases for a specific product will be updated, columns removed or added, tables renamed or removed and so on. When these changes occur it can prevent software designed to process a specific SQLite database from working correctly or produce incorrect results.

- Simple Calculation: Quantity of SQLite databases to analyse **x** Using the correct tool for each database **x** Time to Process each database **x** Review each database **= A LOT OF WASTED TIME!**

 

## Solution

***Template processing*** SQLite databases is an automated method of ***batch*** processing SQLite databases for end user review. First correctly identify each SQLite Database by user configurable identification of internal and external file properties then process each table and each column in the correct matter with as little user intervention as possible.

1. Correctly identify each database – this must be user configurable! If a new SQLite database is encountered then allow the user to identify characteristics associated with the given database. For example: File header and internal settings of SQLite database.

2. Correctly process each table in turn and columns within each table for a particular SQLite database – this must be user configurable! If a new SQLite database is encountered or a small variation occurs in an existing database the user can create a new template to deal with this. At this stage custom queries can be devised to filter and/or present data in a similar fashion to that presented to the user as originally intended.

- **There are infinite variations of how a table in a SQLite database can be laid out. How the data is actually stored within each column is typically only limited to a handful of data types.**

## SQLite Forensic Reporter in a Nutshell

SQLite Forensic Reporter allows you to process virtually any SQLite database using predefined templates. SQLite Forensic Reporter is **template driven** and **fully user configurable** which means when a new SQLite database is identified a new template is created **by the user**. Columns are processed correctly and decoded if required using built in processing routines for date/time formats etc. The user has full control and does not need to wait for an update from the software developer. SQLite Forensic Reporter batch processes SQLite database en-masse greatly reducing the time to extract and present data from SQLite databases present in both computer and mobile devices.

For more information: http://www.filesig.co.uk/sqlite-forensic-reporter.html

**SQLite Forensic Reporter** is **$125USD** per license and priced to be affordable to both individual and organisations alike.