Advanced SQLite and Application Analysis

Advanced• Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

This three day course provides the knowledge and skills necessary for a mobile device examiner to gain an understanding of the SQLite database structure, B-Tree pages and how records are stored within them, SQLite logical structure, and SQLite queries which will allow examiners to extract and format the information contained within the database. Common applications will be used as practical examples giving the examiner a familiarity with mobile device applications that may be encountered frequently in examinations.

Prerequisites:
To obtain the maximum benefit from this class, you should meet the following requirements:

- Able to understand course curriculum presented in English
- Be familiar with Hexadecimal and Binary conversions
- Be familiar with common forensic terminology and concepts
- Be familiar with the Microsoft Windows environment

Class Materials and Software:
You will receive the associated materials prior to the course or arrival at the classroom.

During this three-day, hands-on class, participants will review the following:

- Overview of SQLite
- ACID compliance
- SQLite's use of B-Tree page structure
- Logical data structures of SQLite
- SQLite header deconstruction
- SQLite Query Language
- Recovery of deleted records
- SQLite's implementation in commonly used mobile applications
- Verification of findings

The class includes multiple hands-on labs that allow students to apply what they have learned in the workshop.

(Continued on other side)

SYNTRICATE

SQLite Databases and Application Analysis

Advanced• Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

(Continued)

Module 1: Introduction

Topics:

- Software discussed in this course
  - Vendor Specific
  - Open Source Tools
  - Task Specific Utilities
- Course Overview

Module 2: Introduction to SQLite

Objectives:

- Define SQLite Databases
- Discuss where SQLite databases are used
- Discuss ACID compliance
- Identify SQLite file characteristics
- Discuss Rollback Journal
- Discuss Write Ahead Log (WAL)

Module 3: Looking at the Data

Objectives:

- Search Schema, tables, columns and rows
- Discuss keys and relational elements
- Define the various datatypes native to SQLite
- Compare differences between SQLite and SQL
- Practice finding information within a database
- Practice converting times using Microsoft Excel

Module 4: How SQLite Works: The Hex View

Objectives:

- Decode the Magic Header
- Discuss B-Tree Page Structure
- Decode B-Tree Page Header
- Examine Cells and Decode Cell Header
- Practice decoding each header type

Module 5: Rollback and WAL: The Hex View

Objectives:

- Explore the Locking process with Rollback Journal
- Discuss the reading and writing operations
- Discuss Order of operations with Rollback Journal
- Discuss Hot Journals
- Decode the Rollback Journal page header
- Examine the Locking process with WAL
- Discuss Checkpointing
- Analyze the WAL Header
- Decode WAL Frame
- Practice decoding Rollback Journal and WAL files

Module 6: SQLite Queries

Objectives:

- Discuss naming syntax and order of operations
- Write SELECT statements using:
- WHERE statements for data filtering
- ORDER statements for organization
- JOIN statements for two table joins
- JOIN statements for three or more table joins
- ALIAS statements for changing column names
- Practice writing queries using various tools to retrieve information from various applications

SYNTRICATE

SQLite Database and Application Analysis

Advanced • Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

(Continued)

Module 7: Calculations and Conversions

Objectives:

- Learn the basic operators supported
- Discuss operator organization
- Modify WHERE statements using operators
- Convert timestamps in SQLite queries
- Convert durations in SQLite queries
- Learn how to CAST columns to different data types
- Practice the concepts learned in this module

Module 8: Deleted Records

Objectives:

- Explore Freeblocks
- Decode Freeblock headers in Hex
- Recover deleted records from Rollback and WAL
- Discuss Freespace Pages
- Practice recovering deleted records from SQLite

Module 9: Formatting and Reporting

Objectives:

- Learn the CASE statement to find and replace
- Discuss column name formatting using the AS statement
- Discuss various exporting formats
- Develop Excel Macros for rapid formatting
- Explore MPE+ Reporting Features
- Practice creating reports from the saved queries

SYNTRICATE