COURSE DESCRIPTION

SQLite Forensics Fundamentals

Course Overview

SQLite is a relational database management system which is the most popular format for application developers due to its standalone functionality and ease of setup, management and low resource usage. Most mobile applications have built in SQLite databases to store user data, along with the main web browsers that we use daily. With the release of Windows 10 we have also seen Microsoft adopt SQLite to store data for applications such as TimeLine, the Photo App and Microsoft OneDrive. With this widespread popularity it has become more important that examiners understand the structure of this database format and how to extract and report on information stored within the tables, that our forensic tools may not support.

This course will give participants an understanding of SQLite, how data is stored and the skills necessary to create queries to extract, interpret and present information in a meaningful manner. This includes translating dates and times and querying information stored in multiple tables to create more robust reports.

Course Type
Specialized

Course Length
2 day

Course Code
Spec. – SQLite

What You Will Learn

- Introduction to SQLite
  - This module will introduce you to the SQLite Database and how it has been implemented by the applications that we use on a daily basis.
- SQLite Database Structures, Journal files and Database Schemas
  - These modules will give you an understanding of the structure of the main database file, the Rollback Journal and Write Ahead Logs. We will also look at the schema, and the different types of data stored in the tables.
- SQLite Querying Language
  - This module will provide you with the knowledge to construct queries to extract, interpret and create more robust reports from multiple database tables.
- Exercises on SQLite Databases
  - Using the skills learnt in previous modules we will decode and interrogate the Microsoft Edge Chromium and Mozilla Thunderbird SQLite databases.