SQLite Forensics - More Important Than Ever!

Fill The Gap In Your Mobile Digital Forensics...

Understanding SQLite databases and how to recover data from them is an increasingly essential skillset for digital forensic examiners today. As Apple and Google continue to dominate the Smartphone market, and the ever-increasing number of Apps occupy devices, forensic examiners are regularly confronted with data not supported by the commercial tools.

At present, the most popular mobile forensic tool only supports parsing of less than 300 different applications. This support accounts for a miniscule .001% of the total apps on the market, and leaves a 99.999% gap!

Although Apple and Google devices and their file systems are significantly different, both share a commonality in that they both store a majority of their user data within a data storage container type called SQLite. SQLite is an in-process library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine.

Mobile Forensic Analysts can easily leverage this commonality by learning the skills required to perform low-level analysis and recovery on SQLite databases. Once learned and mastered, examiners can then support nearly 99% of the device data they will come across in the majority of their mobile device examinations. The TeelTech Intro to SQLite Course Will Help Examiners Close the Gap by teaching the fundamentals of SQLite and how to use tools and techniques to recover useful data.

Course Highlights:

- How SQLite works at the byte-level
- What are the different types of SQLite data components
- What are the 5 common locations to recover SQLite data
- How to perform report data validation
- How to Reverse Engineer ANY SQLite database
- Converting and identifying virtually any date format easily
- Display BLOB data within the forensic tool
- How to use a tool designed from the ground-up as a forensic tool
- How to recover data from .SHM, .WAL and .journal files
- How to generate reports quickly from any SQLite database to include external linked images

Students Receive with Class:

- ***A free one-year license of Sanderson Forensics SQLite Forensic Toolkit Software***

Course Creator: Sam Brothers

Sam Brothers is current Digital Forensic Specialist who formerally worked for a US Federal Law Enforcement Agency. He has been in the IT field for over 30 years, and currently specializes in the field of Mobile Device Forensics. He has completed analysis work on hundreds of mobile and computer forensics cases. He and his team had the honor of briefing the then DHS Deputy Secretary on their accomplishments and digital forensic capabilities. He enjoys the opportunity to teach forensic analysis for various law enforcement organizations both in the US and around the world.

Taking the course online.

An instructor will go through the course with you online so you can take it from anywhere. The online version of the course comes in two parts: fundamentals and advanced. Each part is 5 days long. Each day consists of 4 hours of instruction typically held in the morning. You can register for the fundamentals portion, the advanced portion, or the complete course which includes both fundamentals and advanced portions. You cannot take the advanced portion without taking the fundamentals portion first.

	Mon	Tue	Wed	Thu	Fri
Week 1 SQLite Fundamentals	9 am 1 pm	9 am 1 pm	9 am 1 pm	9 am 1 pm	9 am 1 pm
Week 2 SQLite Advanced	9 am 1 pm	9 am 1 pm	9 am 1 pm	9 am 1 pm	9 am 1 pm

SQLite Complete

Taking the course on-site.

Join our instructor and other students in a classroom at one of Teel Tech's instruction facilities across the country. The class is 5 days long and each day has 8 hours of instruction.

	Mon	Tue	Wed	Thu	Fri
SQLite On-site	9 am 5 pm	9 am 5 pm	9 am 5 pm	9 am 5 pm	9 am 5 pm

What our students had to say

> This is an excellent course to provide the student with the foundation to develop methodologies to validate the findings of commercial tools that attempt to parse SQLite data. This data may or may not be addressed by the tools and thus when dealing with mobile apps, many of which are not parsed out by tools, or are partially parsed, you will be able to export the "backend" data and have the skills to extract, reconstruct (relationally) and inspect the data. The class touches on the internal structure of the SQLite databases and provides the student with skills investigate the data contained in SQLite databases and corresponding journal and wal files.

> Doing SQLite forensics is like doing analysis in any other investigation. SQLite forensics is more about formulating a good, repeatable query to tell a story.

> The material was well put together and the flow made the learning easy. This definitely reinforced previous learning and knowledge in the SQLite database structure.