

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*
- *A free 30-day license of Andriller software (LE Only)*
- *Thumbdrive with a library of useful scripts used in class, course exercises and materials.*

Course Creator: Sam Brothers

Sam Brothers is current Digital Forensic Specialist who formerly 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.