

October 2022

Test Results for Mobile Device Acquisition Tool:
Aryson SQLite Database Recovery v22.0

Contents

Introduction.....	1
How to Read This Report	1
1 Results Summary	2
2 Testing Environment.....	4
2.1 Execution Environment	4
2.2 SQLite Data	4
3 Test Results.....	5
3.1 SQLite Data Recovery	6

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology's (NIST) Special Programs Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense's Cyber Crime Center, U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, and the DHS' Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT Web site (<https://www.cftt.nist.gov/>).

This document reports the results from testing Aryson SQLite Database Recovery v22.0 for SQLite data recovery including: displaying recovered SQLite database information, identifying, categorizing and reporting Write-Ahead Log (WAL), Rollback Journal data and sequence WAL journal data.

Test results from other tools can be found on the DHS S&T sponsored digital forensics web page, <http://www.dhs.gov/science-and-technology/nist-cftt-reports>.

How to Read This Report

This report is divided into four sections. Section 1 identifies and provides a summary of any significant anomalies observed in the test runs. This section is sufficient for most readers to assess the suitability of the tool for the intended use. Section 2 identifies the mobile devices used for testing. Section 3 lists testing environment, the internal memory data objects used to populate the mobile devices. Section 4 provides an overview of the test case results reported by the tool.

Test Results for SQLite Data Recovery Tool

Tool Tested: Aryson SQLite Database Recovery

Software Version: v22.0

Supplier: Aryson Technologies

Address: 2880 Zanker Road, Suite 203, San Jose, CA 95134

WWW: arysontechnologies.com

1 Results Summary

Aryson SQLite Database Recovery v22.0 was tested for its ability to report recovered SQLite database information. Except for the following anomalies, the tool was able to report and recover all supported data objects completely and accurately.

Header data:

- The type of journal mode i.e., WAL, PERSIST, OFF is not reported.
- The type of encoding for UTF16 i.e., Big Endian (BE) and Little Endian (LE) is not reported.
- The number of pages is not reported.
- The hash values (e.g., MD5, SHA1) for the associated SQLite file are not reported.

Deleted row data:

Deleted records are not reported.

Modified and Deleted row metadata:

The status of records that have been either deleted or modified are not marked by the tool as “deleted” or “modified”

Binary Large Object (BLOB) data:

Binary Large Object (BLOB) data containing graphic files of type: .gif, .heic, .jpg, .pdf, .png, .tiff are not displayed.

Schema data reporting:

Primary key values are not marked as “Primary Key”. Int and Boolean values are marked incorrectly as “Text”.

Note: When importing sqlite database files that are UTF-16BE the following error occurs: “Endian descriptor is corrupted or file is corrupted”. No data is reported.

For more test result details see section 3.

2 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the selected test execution environment, and the data objects populated for SQLite data recovery.

2.1 Execution Environment

Aryson SQLite Database Recovery v22.0 was installed on Windows 10 Pro version 10.0.19044.2130.

2.2 SQLite Data

Aryson SQLite Database Recovery v22.0 was measured by its ability to report recovered SQLite database information. SQLite versions 3.19.0 (Android) and 3.32.3 (iOS) were used when creating the SQLite databases. These versions are the most current versions running on Android and iOS. Table 2 below defines the SQLite data tested per each test case.

Test Case	Data
SFT-01: SQLite header parsing	<i>Page Size (4096, 1024, 8192)</i> <i>Journal Mode Information (WAL, PERSIST, OFF)</i> <i>Number of Pages</i> <i>UTF-8</i> <i>UTF-16LE</i> <i>UTF-16BE</i>
SFT-02: SQLite Schema Reporting	<i>Table Names</i> <i>Column Names per Table</i> <i>Row Information per Table</i>
SFT-03: SQLite Recoverable Rows	<i>Source filename</i> <i>Row Status: Deleted</i> <i>Row Status: Modified</i>
SFT-04: SQLite Data Element Metadata	<i>Source filename</i> <i>Row Status: Deleted</i> <i>Row Status: Modified</i>
SFT-05: SQLite Schema Data Reporting	<i>Primary Key</i> <i>Int</i> <i>Float</i> <i>Text</i> <i>BLOB (bmp, gif, heic, jpg, pdf, png, tiff)</i> <i>Boolean</i>
SFT-06: Recovered Row Metadata	<i>Source Filename</i> <i>Row Status: Deleted</i> <i>Row Status: Modified</i>
SFT-07: SQLite Recovered Data Information	<i>File Offset, length</i> <i>Table name associated with Row</i>

Table 1: SQLite Data Objects

3 Test Results

This section provides the test case results reported by the tool. Section 3.1 identifies the PRAGMA journal mode (i.e., WAL, PERSIST, OFF), test cases and associated data checked within individual test cases.

Toolname was tested for its ability to report recovered SQLite database information.

The *Test Cases* column in sections 3.1 are comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when testing. The results are as follows:

As Expected: the SQLite data recovery tool returned expected test results.

Partial: the SQLite data recovery tool returned some of data.

Not As Expected: the SQLite data recovery tool failed to return expected test results.

Not Applicable (NA): the tool does not provide support.

3.1 SQLite Data Recovery

SQLite data recovery was testing with Aryson SQLite Database Recovery v22.0.

All test cases were successful with the exception of the following.

- The following header related information is not reported: the type of journal mode (i.e., WAL, PERSIST, OFF); the type of encoding: UTF-16BE, UTF16LE; the number of pages and hash values for the associated SQLite file.
- Deleted records are not reported.
- The status of records that have been either deleted or modified are not marked by the tool as “deleted” or “modified”
- Primary key values are not marked as “Primary Key”. Int and Boolean values are marked incorrectly as “Text”.
- Binary Large Object (BLOB) data containing graphic files of type: .gif, .heic, .jpg, .pdf, .png, .tiff not displayed.

Note: When importing sqlite database files that are UTF-16BE the following error occurs: “Endian descriptor is corrupted or file is corrupted”. No data is reported.

See Table 2 below for more details.

**SQLite Data Recovery
Aryson SQLite Database Recovery v22.0**

Test Cases:	WAL	PERSIST	OFF
SFT-01: Header Parsing Page Size	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-01: Header Parsing Journal Mode Info	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-01: Header Parsing Number of Pages	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-01: Header Parsing UTF-8	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-01: Header Parsing UTF-16LE	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-01: Header Parsing UTF-16BE	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-01: Header Parsing	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>

	WAL	PERSIST	OFF
Test Cases:			
Hash Value (MD5, SHA)			
SFT-02: Schema Reporting Table Name	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-02: Schema Reporting Column Name	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-02: Schema Reporting Number of Rows	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-03: Recoverable Rows Deleted	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-03: Recoverable Rows Modified	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-04: Data Element Metadata Reporting (Source filename) Deleted	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-04: Data Element Metadata Reporting (Source filename) Modified	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting Primary Key	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting Int	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting Float	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-05: Schema Data Reporting Text	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-05: Schema Data Reporting BLOB Data: .bmp	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting BLOB data: .gif	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting BLOB Data: .heic	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting BLOB data: .jpg	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>

Test Cases:	WAL	PERSIST	OFF
SFT-05: Schema Data Reporting BLOB data: .pdf	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting BLOB data: .png	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-05: Schema Data Reporting Boolean	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
SFT-06: Recovered Row Metadata Source Filename	<i>NA</i>	<i>NA</i>	<i>NA</i>
SFT-06: Recovered Row Metadata Status: Modified	<i>NA</i>	<i>NA</i>	<i>NA</i>
SFT-06: Recovered Row Metadata Status: Deleted	<i>NA</i>	<i>NA</i>	<i>NA</i>
SFT-07: Recovered Data Info File offset	<i>NA</i>	<i>NA</i>	<i>NA</i>
SFT-07: Recovered Data Info Recovered Row - Table Name	<i>NA</i>	<i>NA</i>	<i>NA</i>

Table 2: SQLite Data Recovery