June 2023

Test Results for Mobile Device Acquisition Tool:
Belkasoft Evidence Center X v1.17.12873

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security's (DHS) Science and Technology Directorate, 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 Cyber Crime Center, U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, and U.S. 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 website (https://www.cftt.nist.gov/).

This document reports the results from testing Belkasoft Evidence Center X v1.17.12873 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 DHS's computer forensics webpage at https://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 the 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: Belkasoft Evidence Center X

Software Version: v1.17.12873

Supplier: Belkasoft

Address: 702 San Conrado Terrace, Unit 1

Sunnyvale, CA 94085 USA

Phone: +1 (650) 272-0384 (USA and Canada)

Email: sales@belkasoft.com

WWW: https://belkasoft.com/x

1 Results Summary

Belkasoft Evidence Center X v1.17.12873 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.

SQLite header parsing:

PRAGMA journal mode = PERSIST is reported as Rollbackjournal.

Recoverable Rows:

Deleted and modified rows are reported but not identified as such.

Data Element Metadata Reporting (Source filename):

Source filename (db, journal, wal) is not reported for deleted and modified rows.

Schema Data Reporting:

- Data of type "float," is reported as "single."
- BLOB data is reported as type "byte," no content is reported.

Recovered Data Info:

File offset of recovered rows is not 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

Belkasoft Evidence Center X v1.17.12873 was installed on Windows 10 Pro for workstation version 10.0.19044.19044.

2.2 SQLite Data

Belkasoft Evidence Center X v1.17.12873 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	*Page Size (4096, 1024, 8192)* *Journal Mode Information (WAL, PERSIST, OFF)* *Number of Pages* *UTF-8* *UTF-16LE* *UTF-16BE*
SFT-02: SQLite Schema Reporting	*Table Names* *Column Names per Table* *Row Information per Table*
SFT-03: SQLite Recoverable Rows	*Source filename* *Row Status: Deleted* *Row Status: Modified*
SFT-04: SQLite Data Element Metadata	*Source filename* *Row Status: Deleted* *Row Status: Modified*
SFT-05: SQLite Schema Data Reporting	*Primary Key* *Int* *Float* *Text* *BLOB (bmp, gif, heic, jpg, pdf, png, tiff)* *Boolean*
SFT-06: Recovered Row Metadata	*Source Filename* *Row Status: Deleted* *Row Status: Modified*
SFT-07: SQLite Recovered Data Information	*File Offset, length* *Table name associated with Row*

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.

Belkasoft Evidence Center X v1.17.12873 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 Belkasoft Evidence Center X v1.17.12873.

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

- Header parsing information (Journal mode type PERSIST) is reported as Rollbackjournal.
- Deleted and modified rows are reported but not identified as deleted nor modified.
- The source filename (db, journal, wal) for deleted and modified records is not reported.
- Data type "float" is reported as "single."
- Files embedded in a BLOB are not displayed and the data type reported is "byte" instead of BLOB or the file extension.
- File offset of recoverable data is not reported.

See Table 2 below for more details.

SQLite Data Recovery
Belkasoft Evidence Center v1.17.12873

Test Cases:	WAL	PERSIST	OFF
SFT-01: Header Parsing Page Size	*As Expected*	*As Expected*	*As Expected*
SFT-01: Header Parsing Journal Mode Info	*As Expected*	*Not As Expected*	*As Expected*
SFT-01: Header Parsing Number of Pages	*As Expected*	*As Expected*	*As Expected*
SFT-01: Header Parsing UTF-8	*As Expected*	*As Expected*	*As Expected*
SFT-01: Header Parsing UTF-16LE	*As Expected*	*As Expected*	*As Expected*
SFT-01: Header Parsing UTF-16BE	*As Expected*	*As Expected*	*As Expected*
SFT-01: Header Parsing Hash Value (MD5, SHA)	*As Expected*	*As Expected*	*As Expected*
SFT-02: Schema Reporting Table Name	*As Expected*	*As Expected*	*As Expected*
SFT-02: Schema Reporting	*As Expected*	*As Expected*	*As Expected*

Test Cases:	WAL	PERSIST	OFF
Column Name			
SFT-02: **Schema Reporting** Number of Rows	*As Expected*	*As Expected*	*As Expected*
SFT-03: **Recoverable Rows** Deleted	*As Expected*	*As Expected*	*As Expected*
SFT-03: **Recoverable Rows** Modified	*As Expected*	*As Expected*	*As Expected*
SFT-04: **Data Element Metadata Reporting (Source filename)** Deleted	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-04: **Data Element Metadata Reporting (Source filename)** Modified	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting** Primary Key	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** Int	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** Float	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting** Text	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** BLOB Data: .bmp	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting** BLOB data: .gif	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting** BLOB Data: .heic	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting** BLOB data: .jpg	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting** BLOB data: .pdf	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting** BLOB data: .png	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: **Schema Data Reporting**	*As Expected*	*As Expected*	*As Expected*

Test Cases:	WAL	PERSIST	OFF
Boolean			
SFT-06: Recovered Row Metadata Source Filename	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-06: Recovered Row Metadata Status: Modified	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-06: Recovered Row Metadata Status: Deleted	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-07: Recovered Data Info File offset	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-07: Recovered Data Info Recovered Row - Table Name	*As Expected*	*As Expected*	*As Expected*

Table 2: SQLite Data Recovery