

January 2022

Test Results for SQLite Data Recovery Tool:
NUIX Workstation v9.6.5.283

Contents

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

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology (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, as well as the DHS Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and the 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 NUIX Workstation v9.6.5.283 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 S&T-sponsored digital forensics web page, <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 lists testing environment and SQLite data objects used for testing. Section 3 provides an overview of the test case results reported by the tool.

Test Results for SQLite Data Recovery

Tool Tested: NUIX Workstation

Software Version: 9.6.5.283

Supplier: NUIX

Address: 13755 Sunrise Valley Drive, Suite 300, Herndon VA 20171

WWW: nuix.com

1 Results Summary

NUIX Workstation v9.6.5.283 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.

Modified row metadata:

The status of records that have been modified are not specified by the tool as “modified” records.

Binary Large Object data:

Binary Large Object (BLOB) data containing graphic files of type: .pdf are not displayed.

For more test result details see section 2.

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

NUIX Workstation was installed on Windows 10 Pro version 10.0.18363.418.

2.2 SQLite Data

NUIX Workstation v9.6.5.283 was measured by its ability to report recovered SQLite database information. SQLite versions 3.19.0 (Android) and 3.32.3 iPhone Operating System (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
SQLite Forensic Tool (SFT)-01: SQLite header parsing	<i>Page Size (4096, 1024, 8192)</i> <i>Journal Mode Information (Write-Ahead Log (WAL), PERSIST, OFF)</i> <i>Number of Pages</i> <i>UTF (Unicode Transformation Format)-8</i> <i>UTF-16 (Little Endian) LE</i> <i>UTF-16 (Big Endian) BE</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>Integer (Int)Float</i> <i>Text</i> <i>Binary Large Object (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.

NUIX Workstation v9.6.5.283 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 the data.

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

Not Applicable (NA): the tool does not provide support, or the test assertion is optional.

3.1 SQLite Data Recovery

SQLite data recovery was tested with NUIX Workstation v9.6.5.283.

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

- The status of records that have been modified are not specified by the tool as “modified” records.
- BLOB data containing graphic files of type: .pdf are not displayed.
- **NOTE:** NUIX does not provide support for reporting the following information associated with SQLite database files: Page Size: 1024, 4096, 8192; Journal Mode: WAL, PERSIST, OFF; Number of Pages, Page Encoding: UTF8, UTF16LE, UTF16BE, deleted records. Therefore, the fields for these data types in Table 2 are marked as Not Applicable (NA).

See Table 2 below for more details.

NUIX Workstation v9.6.5.283				
Test Cases – SQLite Data Recovery		PRAGMA Journal Mode		
		WAL	PERSIST	OFF
SFT-01: Header Parsing	Page Size	NA	NA	NA
	Journal	NA	NA	NA
	Number of	NA	NA	NA
	UTF-8	NA	NA	NA
	UTF-16LE	NA	NA	NA
	UTF-16BE	NA	NA	NA
	Hash Value	As Expected	As Expected	As Expected
SFT-02: Schema Reporting	Table	As Expected	As Expected	As Expected
	Column Name	As Expected	As Expected	As Expected
	Number of Rows	As Expected	As Expected	As Expected
SFT-03: Recoverable Rows	Deleted	NA	NA	NA
	Modified	As Expected	As Expected	As Expected
SFT-04: Data Element Metadata Reporting (Source filename)	Deleted	NA	NA	NA
	Modified	Not As Expected	Not As Expected	Not As Expected
SFT-05: Schema Data Reporting	Primary	As Expected	As Expected	As Expected
	Int	As Expected	As Expected	As Expected
	Float	As Expected	As Expected	As Expected
	Text	As Expected	As Expected	As Expected
	BLOB Data: .bmp	As Expected	As Expected	As Expected
	BLOB data: .gif	As Expected	As Expected	As Expected
	BLOB Data: .heic	As Expected	As Expected	As Expected

NUIX Workstation v9.6.5.283				
Test Cases – SQLite Data Recovery		PRAGMA Journal Mode		
		WAL	PERSIST	OFF
	BLOB data: .jpg	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	BLOB data: .pdf	<i>Not As Expected</i>	<i>Not As Expected</i>	<i>Not As Expected</i>
	BLOB data: .png	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	Boolean	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SFT-06: Recovered Row Metadata	Source Filename	<i>NA</i>	<i>NA</i>	<i>NA</i>
	Status: Modified	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	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>
	Recovered Row - Table Name	<i>NA</i>	<i>NA</i>	<i>NA</i>

Table 2: SQLite Data Recovery