November 2022

Test Results for Mobile Device Acquisition Tool:
NUIX Workstation v9.10.5.374

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 (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 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 objective 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 v9.10.5.374 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 at 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 the testing environment and 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: NUIX Workstation

Software Version: v9.10.5.374

Supplier: NUIX

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

WWW: nuix.com

1 Results Summary

NUIX Workstation v9.10.5.374 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.

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

NUIX Workstation v9.10.5.374 was installed on a Windows 10 Pro version 10.0.14393 computer.

2.2 SQLite Data

NUIX Workstation v9.10.5.374 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 1 below defines the SQLite data tested per 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.

NUIX Workstation v9.10.5.374 was tested for its ability to report recovered SQLite database information.

The *Test Cases* column in Section 3.1 are comprised of two sub-columns that define a particular test category and individual subcategories 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 tested with NUIX Workstation v9.10.5.374.

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

> The status of records that have been modified are not specified y the tool as "modified" records.

> ***NOTE:*** NUIX does not provide support for reporting the following information associated with SQLite database files: Page Size: 1024, 4096, 8192; Journal Mode: WAL, PERSIT, 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:

SQLite Data Recovery
NUIX Workstation v9.10.5.374

Test Cases:	WAL	PERSIST	OFF
SFT-01: **Header Parsing** Page Size	*NA*	*NA*	*NA*
SFT-01: **Header Parsing** Journal Mode Info	*NA*	*NA*	*NA*
SFT-01: **Header Parsing** Number of Pages	*NA*	*NA*	*NA*
SFT-01: **Header Parsing** UTF-8	*NA*	*NA*	*NA*
SFT-01: **Header Parsing** UTF-16LE	*NA*	*NA*	*NA*
SFT-01: **Header Parsing** UTF-16BE	*NA*	*NA*	*NA*
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*

Test Cases:	WAL	PERSIST	OFF
SFT-02: **Schema Reporting** Column Name	*As Expected*	*As Expected*	*As Expected*
SFT-02: **Schema Reporting** Number of Rows	*As Expected*	*As Expected*	*As Expected*
SFT-03: **Recoverable Rows** Deleted	*NA*	*NA*	*NA*
SFT-03: **Recoverable Rows** Modified	*As Expected*	*As Expected*	*As Expected*
SFT-04: **Data Element Metadata Reporting (Source filename)** Deleted	*NA*	*NA*	*NA*
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	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** Text	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** BLOB Data: .bmp	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** BLOB data: .gif	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** BLOB Data: .heic	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** BLOB data: .jpg	*As Expected*	*As Expected*	*As Expected*
SFT-05: **Schema Data Reporting** BLOB data: .pdf	*As Expected*	*As Expected*	*As Expected*

Test Cases:	WAL	PERSIST	OFF
SFT-05: Schema Data Reporting BLOB data: .png	*As Expected*	*As Expected*	*As Expected*
SFT-05: Schema Data Reporting Boolean	*As Expected*	*As Expected*	*As Expected*
SFT-06: Recovered Row Metadata Source Filename	*As Expected*	*As Expected*	*As Expected*
SFT-06: Recovered Row Metadata Status: Modified	*As Expected*	*As Expected*	*As Expected*
SFT-06: Recovered Row Metadata Status: Deleted	*NA*	*NA*	*NA*
SFT-07: Recovered Data Info File offset	*NA*	*NA*	*NA*
SFT-07: Recovered Data Info Recovered Row - Table Name	*NA*	*NA*	*NA*

Table 2: SQLite Data Recovery