November 2021

Test Results for SQLite Data Recovery Tool:
Forensic Toolkit (FTK) v7.5.1.127

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, the National Institute of Justice (NIJ), and the National Institute of Standards and Technology (NIST) Special Programs Office and Information Technology Laboratory (ITL). 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 Criminal Investigation Division Electronic Crimes Program, and DHS's 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 Exterro's FTK v7.5.1.127 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:	FTK
Software Version:	7.5.1.127
Supplier:	Exterro
Address:	4145 SW Watson Ave., Suite 400 Beaverton, OR 97005
Tel:	503-501-5100
WWW:	exterro.com/forensic-toolkit

1 Results Summary

FTK v7.5.1.127 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.

Deleted data reporting:

- Deleted records that are recoverable are not reported.

Recovered 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 2.

2 Testing Environment

The tests were run in the National Institute of Standards and Technology (NIST) CFTT lab. This section describes the selected test execution environment, and the data objects populated for SQLite data recovery.

2.1 Execution Environment

FTK v7.5.1.127 v9.6 was installed on Windows 10 Pro version 10.0.14393.

2.2 SQLite Data

FTK v7.1.1.237 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	*Page Size (4096, 1024, 8192)*
	Journal Mode Information (Write-Ahead Log (WAL), PERSIST, OFF)
	Number of Pages
	UTF(Unicode Transformation Format)-8
	UTF-16 (Little Endian) LE
	UTF-16 (Big Endian) BE
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*
	Integer (Int)
	Float
	Text
	Binary Large Object (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.

FTK v7.5.1.127 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 or the test assertion is optional.

3.1 SQLite Data Recovery

SQLite data recovery was testing with FTK v7.5.1.127.

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

- Deleted records that are recoverable are not reported.
- The status of records that have been modified are not specified by the tool as "modified" records.

See Table 2 below for more details.

FTK v7.5.1.127				
Test Cases – SQLite Data Recovery		*PRAGMA Journal Mode*		
		WAL	PERSIST	OFF
SFT-01: Header Parsing	Page Size	*NA*	*NA*	*NA*
	Journal Mode Info	*NA*	*NA*	*NA*
	Number of Pages	*NA*	*NA*	*NA*
	UTF-8	*NA*	*NA*	*NA*
	UTF-16LE	*NA*	*NA*	*NA*
	UTF-16BE	*NA*	*NA*	*NA*
	Hash Value (MD5, SHA)	*As Expected*	*As Expected*	*As Expected*
SFT-02: Schema Reporting	Table Name	*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	*Not As Expected*	*Not As Expected*	*Not As Expected*
	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 Key	*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*

FTK v7.5.1.127				
Test Cases – SQLite Data Recovery		*PRAGMA Journal Mode*		
		WAL	PERSIST	OFF
	BLOB data: .gif	*As Expected*	*As Expected*	*As Expected*
	BLOB Data: .heic	*As Expected*	*As Expected*	*As Expected*
	BLOB data: .jpg	*As Expected*	*As Expected*	*As Expected*
	BLOB data: .pdf	*As Expected*	*As Expected*	*As Expected*
	BLOB data: .png	*As Expected*	*As Expected*	*As Expected*
	Boolean	*As Expected*	*As Expected*	*As Expected*
SFT-06: Recovered Row Metadata	Source Filename	*NA*	*NA*	*NA*
	Status: Modified	*NA*	*NA*	*NA*
	Status: Deleted	*NA*	*NA*	*NA*
SFT-07: Recovered Data Info	File offset	*NA*	*NA*	*NA*
	Recovered Row - Table Name	*NA*	*NA*	*NA*

Table 2: SQLite Data Recovery