October 2021

Test Results for Mobile Device Acquisition Tool:
Belkasoft X Version 1.10.8387

Federated Testing Suite for Mobile Device Acquisition

Contents

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 Belkasoft X Version 1.10.8387 using the CFTT Federated Testing Test Suite for Mobile Device Acquisition, Version 5.

Federated Testing is an expansion of the CFTT program to provide forensic investigators and labs with test materials for tool testing and to support shared test reports. The goal of Federated Testing is to help forensic investigators to test the tools that they use in their labs and to enable sharing of tool test results. CFTT's Federated Testing Forensic Tool Testing Environment and included test suites can be downloaded from http://www.cftt.nist.gov/federated-testing.html and used to test forensic tools. The results can be optionally shared with CFTT, reviewed by CFTT staff, and then shared with the community.

Test results from other tools can be found on DHS's computer forensics web page, https://www.dhs.gov/science-and-technology/nist-cftt-reports.

How to Read This Report

This report is organized into the following sections:

1. Tested Tool Description. The tool name, version and vendor information are listed.
2. Testing Organization. Contact information and approvals.
3. How to Read This Report (this section).
4. Results Summary. This section identifies any significant anomalies observed in the test runs. This section provides a narrative of key findings identifying where the tool meets expectations and provides a summary of any ways the tool did not meet expectations. The section also provides any observations of interest about the tool or about testing the tool including any observed limitations or organization-imposed restrictions on tool use.
5. Test Environment. Description of hardware and software used in tool testing in sufficient detail to satisfy the testing organization's policy and requirements.
6. Mobile Devices Used in Testing. A table describing each mobile device used in testing. Includes the make, model, operating system, firmware version and network of each device.
7. Device Setup. List of data elements populated to each device.
8. Test Result Details by Device.

Federated Testing Test Results for Mobile Device Acquisition Tool: Belkasoft X Version 1.10.8387

Tool Description

Tool Name:	Belkasoft X
Tool Version:	1.10.8387
Vendor:	Belkasoft LLC

Testing Organization

Organization conducting test: Belkasoft LLC
Contact: support@belkasoft.com
Report date: October 1, 2021
Authored by: Anton

This test report was generated using CFTT's Federated Testing Forensic Tool Testing Environment, see Federated Testing Home Page.

Results Summary

Two different acquisition methods were used to get a full file system image of the testing device. Both images were then analyzed, and the extracted data were compared with the expected results and cross-checked. Found issues were fixed, and the whole process was iterated until all discrepancies had been accommodated, and the tool met expectations.

Test Environment

This section describes any additional hardware or software used in testing.

Hardware: a desktop based on ASUSTeK PRIME H310-PLUS, with Intel Core i5-8500 CPU, 16 Gb RAM and USB 3.0 ports, under Windows 10 build 19043. A proprietary USB key required to authorize iOS acquisition with the tested product. An original Apple cable.

Software: Microsoft Store's iTunes.

Mobile Devices Used in Testing

The following table lists the mobile devices used in testing Belkasoft X Version 1.10.8387.

Mobile Devices Used in Testing Belkasoft X Version 1.10.8387

Make	Model	OS	Version	Firmware	Network	SIM/UICC
Apple	iPhone 8 Plus MQ6G2RU/A	iOS	13.4.1		GSM	No SIM/UICC

Device Setup

The following sections describe the data objects populated onto the internal memory of the test mobile devices.

Setup for iOS Devices

Setup for iOS Devices

Data Objects		Apple iPhone 8 Plus MQ6G2RU/A
PIM Data: Contacts/Address Book Entries	Regular Length	populated
	Maximum Length	populated
	Special Character	populated
	Blank Name	populated
	Regular Length, email	populated
	Regular Length, graphic	populated
	Regular Length, Address	populated
	Non-Latin Entry	populated
	Contact Groups	omitted
	Deleted Entry	populated
PIM Data: Calendar, Memos	Regular Length	populated
	Maximum Length	populated
	Special Character	populated
	Blank Entry	populated
	Deleted Entry	populated
Stand-Alone Data Files	Audio	populated
	Graphic	populated
	Video	populated
	Documents	populated
	Audio – Deleted	omitted
	Graphic - Deleted	omitted
	Video – Deleted	omitted
	Documents - Deleted	omitted
Call Logs	Incoming	populated
	Outgoing	populated
	Missed	populated
	Incoming – Deleted	populated
	Outgoing – Deleted	populated
	Missed – Deleted	populated
SMS/EMS Messages	Incoming SMS – Read	populated

	Incoming SMS – Unread	populated
	Incoming SMS – Deleted	omitted
	Incoming EMS – Read	omitted
	Incoming EMS – Unread	omitted
	Incoming EMS – Deleted	omitted
	Outgoing SMS	populated
	Outgoing Group SMS	omitted
	Outgoing SMS – Deleted	omitted
	Outgoing EMS	omitted
	Outgoing Group EMS	omitted
	Outgoing EMS – Deleted	omitted
MMS Messages	Incoming Audio	omitted
	Incoming Graphic	populated
	Incoming Video	omitted
	Outgoing Audio	omitted
	Outgoing Graphic	omitted
	Outgoing Video	omitted
Location Data	GPS Coordinates	populated
	Geo-tagged Data	populated
Browser/Email Data	Visited Sites	populated
	Bookmarks	populated
	Email	populated
Social Media Data	Application 1, e.g., Facebook	populated
	Application 2, e.g., Twitter	populated
	Application 3, e.g., LinkedIn	populated
	Application 4, e.g., Instagram	populated
Other Applications of Interest	Other Applications of Interest	populated

Test Results

This section provides the test results from testing Belkasoft X Version 1.10.8387.

The Test Results column (Internal Memory Acquisition) in the following subsections are composed of two sub-columns that define a particular test category and individual sub-categories that are verified when acquiring the internal memory for supported mobile devices. Each individual sub-category row shows results for each mobile device tested. The results are as follows:

As Expected: the mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device or SIM/UICC successfully.

Partial: the mobile forensic application returned some of data from the mobile device or SIM/UICC.

Not As Expected: the mobile forensic application failed to return expected test results – the tool did not acquire or report supported data from the mobile device or SIM/UICC successfully.

NA: Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element.

Results for iOS Devices

Test Results -- Internal Memory Acquisition		AppleiPhone 8 Plus MQ6G2RU/A
Acquisition	Acquire All	as expected
	Disrupted	as expected
Reporting	Preview-Pane	as expected
	Generated Reports	as expected
Equipment/User Data	IMEI	N/A
	MEID/ESN	N/A
	MSISDN/MIN	N/A
PIM Data	Contacts	as expected
	Calendar	as expected
	Memos/Notes	as expected
Stand-Alone Data Files	Audio	as expected
	Graphic	as expected
	Video	as expected
	Documents	as expected
Call Logs	Incoming	as expected
	Outgoing	as expected

	Missed	as expected
SMS/EMS Messages	Incoming	as expected
	Outgoing	as expected
MMS Messages	Audio	N/A
	Graphic	as expected
	Video	N/A
Location Data	Coordinates/Geo-tagged	as expected
Browser/Email Data	Visited Sites	as expected
	Bookmarks	as expected
	Email	as expected
Social Media Data	Application 1, e.g., Facebook	as expected
	Application 2, e.g., Twitter	as expected
	Application 3, e.g., LinkedIn	as expected
	Application 4, e.g., Instagram	as expected
Other Applications of Interest	Other Applications of Interest	as expected
Non-Latin Character	Reported in native format	as expected
Hashing	Case File/Individual Files	N/A
Case File Data Protection	Modify Case Data	N/A

Tool: @(#) ft_mdt_prt_test_report.py Version 1.2 created 04/26/18 at 10:11:19
OS: Linux Version 4.13.0-37-generic
Federated Testing Version 5, released 3/12/2020

Test Setup & Analysis Tool Versions

Version numbers of tools used are listed.

Setup & Analysis Tool Versions

cftt-di Version 1.25 created 05/23/18 at 15:58:45
diskwipe.c Linux Version 1.5 Created 03/20/13 at 14:23:34

Tool: @(#) ft-di-prt_test_report.py Version 1.24 created 05/23/18 at 16:08:06
OS: Linux Version 4.13.0-37-generic
Federated Testing Version 5, released 3/12/2020