

February 2022

Test Results for Mobile Device Acquisition Tool:
Graykey OS v1.7.3.19461530 App Bundle v2.2.2

Contents

Introduction.....	1
How to Read This Report	1
1 Results Summary	3
2 Mobile Devices	4
3 Testing Environment.....	4
3.1 Execution Environment	4
3.2 Internal Memory Data Objects.....	4
4 Test Results.....	7
4.1 iOS Mobile Devices.....	8

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 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 (<http://www.cftt.nist.gov/>).

This document reports the results from testing Graykey OS v1.7.3.19461530 App bundle v2.2.2 across supported iOS devices.

Test results from other tools can be found on the DHS S&T-sponsored digital forensics webpage, <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 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 Mobile Device Acquisition Tool

Tool Tested: Graykey OS

Software Version: v1.7.3.19461530, App bundle v2.2.2

Supplier: Grayshift LLC

Address: 931 Monroe Drive NE Suite A 102-340, Atlanta, GA 30308

Phone: (833) 472-9539

WWW: grayshift.com

1 Results Summary

Graykey OS v1.7.3.19461530 App bundle v2.2.2 was tested for its ability to acquire active data from the internal memory of supported iOS devices.

Graykey OS v1.7.3.19461530 App bundle v2.2.2 acquired supported data objects completely and accurately for all mobile devices tested.

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing Graykey OS v1.7.3.19461530 App bundle v2.2.2.

Make	Model	OS	Extraction Type	Firmware	Network
Apple iPhone	7	iOS 10.2 (14C92)	Full File System	1.33.00	CDMA
Apple iPhone	8 Plus	iOS 11.4.1 (15G77)	Full File System	1.89.00	CDMA
Apple iPhone	X	iOS 11.3.1 (15E302)	Full File System	1.89.00	CDMA
Apple iPhone	SE	iOS 15.1 (MX9N2LL/A)	Full File System	1.06.00	CDMA
Apple iPhone	11	iOS 15.1 (15E302)	Full File System	3.0.00	CDMA
Apple iPad	Air	iOS 11.2.1 (11D167)	Full File System	2.18.02	CDMA
Apple iPad	Mini	iOS 11.3.1 (15E302)	Full File System	4.52.00	CDMA

Table 1: Mobile Devices

3 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the selected test execution environment, and the data objects populated onto the internal memory of mobile devices.

3.1 Execution Environment

Graykey OS v1.7.3.19461530 App bundle v2.2.2 was installed on Windows 10 Pro version 10.0.19042.1415.

3.2 Internal Memory Data Objects

Graykey OS v1.7.3.19461530 App bundle v2.2.2 was measured by analyzing acquired data from the internal memory of pre-populated mobile devices. Table 2 defines the data objects and elements used for populating mobile devices provided the mobile device supports the data element.

Data Objects	Data Elements
Address Book Entries	<i>Regular Length Maximum Length Special Character Blank Name Regular Length, Email Regular Length, Graphic Regular Length, Address Deleted Entry Non-Latin Entry Contact Groups</i>
PIM Data: Datebook/Calendar; Memos	<i>Regular Length Maximum Length Deleted Entry Special Character Blank Entry</i>
Call Logs	<i>Incoming Outgoing Missed Incoming – Deleted Outgoing – Deleted Missed – Deleted</i>
Text Messages	<i>Incoming SMS – Read Incoming SMS – Unread Outgoing SMS Incoming EMS – Read Incoming EMS – Unread Outgoing EMS Incoming SMS – Deleted Outgoing SMS – Deleted Incoming EMS – Deleted Outgoing EMS – Deleted Non-Latin SMS/EMS</i>
MMS Messages	<i>Incoming Audio Incoming Graphic Incoming Video Outgoing Audio Outgoing Graphic Outgoing Video</i>
Application Data	<i>Device Specific App Data</i>

Data Objects	Data Elements
Stand-alone Data Files	<i>Audio</i> <i>Graphic</i> <i>Video</i> <i>Audio – Deleted</i> <i>Graphic – Deleted</i> <i>Video – Deleted</i>
Internet Data	<i>Visited Sites</i> <i>Bookmarks</i> <i>E-mail</i>
Location Data	<i>GPS Coordinates</i> <i>Geo-tagged Data</i>
Social Media Data	<i>Facebook</i> <i>Twitter</i> <i>LinkedIn</i> <i>Instagram</i> <i>Pinterest</i> <i>SnapChat</i> <i>WhatsApp</i>

Table 2: Internal Memory Data Objects

4 Test Results

This section provides the test cases results reported by the tool. Section 4.1 identifies the mobile device operating system type and the make and model of mobile devices used for testing App bundle v2.2.2.

The *Test Cases* column (internal memory acquisition) in section 4.1 is comprised 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 within each test case. 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 successfully.

Partial: the mobile forensic application returned some data from the mobile device.

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 successfully.

NA: Not Applicable – the tool does not provide support for the acquisition for a particular data element.

4.1 iOS Mobile Devices

The internal memory contents for iOS devices were acquired with Graykey OS v1.7.3.19461530 and analyzed with a third party tool.

All test cases pertaining to the acquisition of supported iOS devices were successful, no anomalies were found.

See Table 3 below for more details.

Graykey OS v1.7.3.19461530

Test Cases – Internal Memory Acquisition		<i>Mobile Device Platform: iOS</i>						
		iPhone 7	iPhone 8 Plus	iPhone X	iPhone SE	iPhone 11	iPad Air v11.2.1	iPad Mini v11.3.1
Acquisition	Acquire All	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Disrupted	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Reporting	Preview-Pane	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Generated Reports	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Equipment/ User Data	IMEI/MEID/ ESN	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	MSISDN	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
PIM Data	Contacts	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Calendar	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Memos/Notes	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Call Logs	Incoming	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	NA	NA
	Outgoing	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	NA	NA
	Missed	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	NA	NA
SMS Messages	Incoming	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Outgoing	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
MMS Messages	Graphic	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Audio	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Video	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Stand-alone Files	Graphic	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Audio	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Video	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Application Data	Documents (txt, pdf files)	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>

Graykey OS v1.7.3.19461530

Test Cases – Internal Memory Acquisition		<i>Mobile Device Platform: iOS</i>						
		<i>iPhone 7</i>	<i>iPhone 8 Plus</i>	<i>iPhone X</i>	<i>iPhone SE</i>	<i>iPhone 11</i>	<i>iPad Air v11.2.1</i>	<i>iPad Mini v11.3.1</i>
Social Media Data	Facebook	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	Twitter	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	LinkedIn	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	Instagram	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	Pinterest	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	SnapChat	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	WhatsApp	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
Internet Data	Bookmarks	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	History	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
	Email	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
GPS Data	Coordinates/Geo-tagged	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
Non-Latin Character	Reported in native format	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
Hashing	Case File/Individual Files	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
Case File Data Protection	Modify Case Data	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>	<i>As Expected</i>
SQLite Data	Report Active Data	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>
	Run SQLite Commands	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>

Table 3: iOS Devices