October 2022

Test Results for Mobile Device Acquisition Tool:
GrayKey Advanced Rev D, Cable B, OS 1.10.1.21812323 App Logic 3.6.0

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 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 Web site (https://www.cftt.nist.gov/).

This document reports the results from testing GrayKey Advanced Rev D, Cable B, OS 1.10.1.21812323 App Logic 3.6.0 across supported Android devices.

Test results from other tools can be found on the DHS S&T sponsored digital forensics web page, 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

Software Version: Rev D, Cable B, OS 1.10.1.21812323 App Logic 3.6.0

Supplier: Grayshift

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

Phone: +1 (833) 472-9539

WWW: grayshift.com

1 Results Summary

GrayKey Rev D, Cable B, OS 1.10.1.21812323 App Logic 3.6.0 was tested for its ability to acquire active data from the internal memory of supported Android devices.

Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Personal Information Management (PIM) Data:

Notes were not reported. (Device: ***Google Pixel 4***)

Social Media Data:

- Social media data for Twitter is not reported. (Device: ***Samsung Galaxy Z Fold 3***)
- Social media data for Snapchat is not reported. (Device: ***Samsung Galaxy Tab S8***)
- Social media data for Twitter and Pinterest) is partially reported i.e., posts and direct messages are not reported, only application related graphic files. (Device: ***Google Pixel 4***)

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing GrayKey Advanced Red D, Cable B, OS 1.10.1.218.12323 App Logic 3.6.0.

Make	Model Name	OS	Model #	Network
Samsung	Galaxy S22	Android 12	SM-S901U1	CDMA
Samsung	Galaxy Z Fold3 5G	Android 12	SM-F926U1	CDMA
Samsung	Galaxy Tab S8	Android 12	SM-X700	CDMA
Google	Pixel 4	Android 10	G0201	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 Advanced Red D, Cable B, OS 1.10.1.218.12323 App Logic 3.6.0 was installed on Windows 10 Pro version 10.0.19042.1586.

3.2 Internal Memory Data Objects

GrayKey Advanced Red D, Cable B, OS 1.10.1.218.12323 App Logic 3.6.0 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	*Regular Length* *Maximum Length* *Special Character* *Blank Name* *Regular Length, email* *Regular Length, graphic* *Regular Length, Address* *Deleted Entry* *Non-Latin Entry* *Contact Groups*
PIM Data: Datebook/Calendar; Memos	*Regular Length* *Maximum Length* *Deleted Entry* *Special Character* *Blank Entry*

Data Objects	Data Elements
Call Logs	*Incoming* *Outgoing* *Missed* *Incoming – Deleted* *Outgoing – Deleted* *Missed - Deleted*
Text Messages	*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*
MMS Messages	*Incoming Audio* *Incoming Graphic* *Incoming Video* *Outgoing Audio* *Outgoing Graphic* *Outgoing Video*
Application Data	*Device Specific App Data*
Stand-alone data files	*Audio* *Graphic* *Video* *Audio – Deleted* *Graphic - Deleted* *Video - Deleted*
Internet Data	*Visited Sites* *Bookmarks* *E-mail*
Location Data	*GPS Coordinates* *Geo-tagged Data*
Social Media Data	*Facebook* *Twitter* *LinkedIn* *Instagram* *Pinterest* *Snapchat* *WhatsApp* *TikTok*

Table 2: Internal Memory Data Objects

4 Test Results

This section provides the test cases results reported by the tool. Sections 4.1 – 4.3 identify the mobile device operating system type, media (e.g., Android, iOS, UICC) and the make and model of mobile devices used for testing GrayKey Advanced Red D, Cable B, OS 1.10.1.218.12323 App Logic 3.6.0.

The *Test Cases* column (internal memory acquisition) in sections 4.1 are 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 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/UICC successfully.

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

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

4.1 Android Mobile Devices

The internal memory contents for Android devices were acquired with GrayKey Advanced Red D, Cable B, OS 1.10.1.218.12323 App Logic 3.6.0. All test cases pertaining to the acquisition of supported Android devices were successful with the exception of the following across all Android devices.

- Notes were not reported for the Google Pixel 4.
- Social media data for Twitter is not reported for the Samsung Galaxy Z Fold 3.
- Social media data for Snapchat is not reported for the Samsung Galaxy Tab S8.
- Social media data (Twitter, Pinterest) is partially reported (i.e., graphic files) for the Google Pixel 4.

See Table 3 below for more details.

Internal Memory Acquisition
GrayKey Advanced Red D, Cable B, OS 1.10.1.218.12323 App Logic 3.6.0
Mobile Device Platform: Android

Test Cases:	Samsung Galaxy S22	Samsung Galaxy Z Fold 3 5G	Samsung Galaxy Tab S8	Google Pixel 4
Acquisition: Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Acquisition: Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Reporting: Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Reporting: Generated Reports	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Equipment/User Data: IMEI/MEID/ESN	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Equipment/User Data: MSISDN	*As Expected*	*As Expected*	*As Expected*	*As Expected*
PIM Data: Contacts	*As Expected*	*As Expected*	*As Expected*	*As Expected*
PIM Data: Calendar	*As Expected*	*As Expected*	*As Expected*	*As Expected*
PIM Data: Memos/Notes	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*
Call Logs: Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Call Logs: Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Call Logs: Missed	*As Expected*	*As Expected*	*As Expected*	*As Expected*
SMS Messages: Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*
SMS Messages: Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages: Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages: Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages: Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Stand-alone Files: Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Stand-alone Files: Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Stand-alone Files: Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application Data: Documents (txt, pdf files)	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Test Cases:	Samsung Galaxy S22	Samsung Galaxy Z Fold 3 5G	Samsung Galaxy Tab S8	Google Pixel 4
Social Media Data: Facebook	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Social Media Data: Twitter	*As Expected*	*Not As Expected*	*As Expected*	*Partial*
Social Media Data: LinkedIn	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Social Media Data: Instagram	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Social Media Data: Pinterest	*As Expected*	*As Expected*	*As Expected*	*Partial*
Social Media Data: Snapchat	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*
Social Media Data: WhatsApp	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Social Media Data: TikTok	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Internet Data: Bookmarks	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Internet Data: History	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Internet Data: Email	*As Expected*	*As Expected*	*As Expected*	*As Expected*
GPS Data: Coordinates/Geo-tagged	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Non-Latin Character: Reported in native format	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Hashing: Case File/ Individual Files	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Case File Data Protection: Modify Case Data	*As Expected*	*As Expected*	*As Expected*	*As Expected*
SQLite Data: Report Active Data	*As Expected*	*As Expected*	*As Expected*	*As Expected*
SQLite Data: Run SQLite Commands	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Table 3: Android Devices