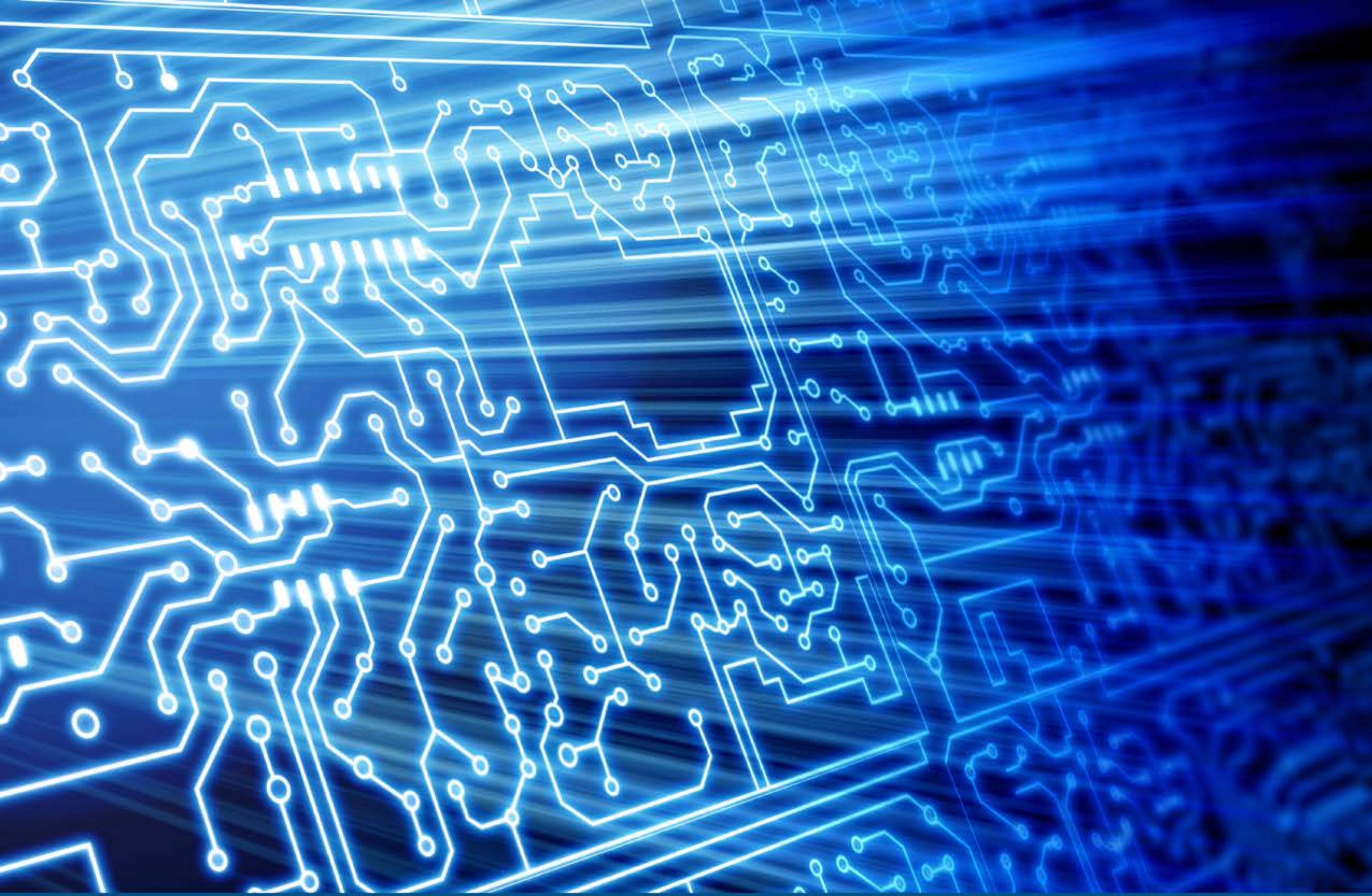

Katana Forensics Triage v1.1802.220

Test Results for Mobile Device Acquisition Tool

May 26, 2018

Homeland Security

Science and Technology

This report was prepared for the Department of Homeland Security Science and Technology Directorate Cyber Security Division by the Office of Law Enforcement Standards of the National Institute of Standards and Technology.

For additional information about the Cyber Security Division and ongoing projects, please visit http://www.dhs.gov/science-and-technology/cyber-security-division.

May 2018

Test Results for Mobile Device Acquisition Tool:
Katana Forensics Triage v1.1802.220

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS), the National Institute of Justice (NIJ), and the National Institute of Standards and Technology Special Program Office (SPO) 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 the U.S. Department of Homeland Security'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 (http://www.cftt.nist.gov/).

This document reports the results from testing Katana Forensics Triage v1.1802.220 across supported mobile devices i.e., Android and iOS.

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:	Katana Forensics Triage
Software Version:	1.1802.220
Supplier:	Katana Forensics
Address:	210 Marlboro Rd Suite 25 PMB 389 Easton, MD 21601
Tel:	(410) 822-7294
WWW:	www.katanaforensics.com

1 Results Summary

Katana Forensics Triage version 1.1802.220 provides examiners with the ability to acquire data on scene. Katana Forensics Triage supports both Windows and macOS computers. Katana Forensics Triage provides examiners with the ability to: view phone and message data simultaneously, call and message visualization, two extraction modes (fast and full) supporting Android 6+ and iOS 8+, iCloud triage support, HTML reporting, CVS exporting, File system export, Case file encryption, Cloud licensing and sharing, Call Detail Records with Geolocation Mapping.

The tool was tested for its ability to acquire active data from the internal memory of supported mobile devices (i.e., Android, iOS). Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

***Connectivity*:**

- When connectivity is disrupted during acquisition an error message is not returned. (Devices: *Android, iOS*)

***Subscriber, Equipment related data*:**

- The MSISDN/MDN and IMEI was not reported. (Devices: *Android*)

***Personal Information Management (PIM) data*:**

- Graphic files associated with Contact/Address book entries are not reported. (Devices: *Android, iOS*)
- Call log status i.e., incoming, outgoing, missed is not reported. (Device: *iPhone 5S*)
- Memo entries are not reported. (Devices: *Ellipsis 8, iPhone 6S Plus, iPhone 7, iPhone 7 Plus, iPad Mini, iPad Pro*)

GPS Related Data:

- No Maps GPS related data (i.e., longitude, latitude) coordinates are reported. (Devices: *Android*)

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing Katana Forensics Triage version 1.1802.220.

Make	Model	OS	Firmware	Network
Apple	iPhone 5S	iOS 7.1 (11D167)	2.18.02	CDMA
Apple	iPhone 6S Plus	iOS 9.2.1 (13C75)	1.23.00	CDMA
Apple	iPhone 7	iOS 10.2 (14C92)	1.33.00	CDMA
Apple	iPhone 7 Plus	iOS 10.2 (14C92)	1.33.00	CDMA
Apple	iPad Mini	iOS 9.2.1 (13B143)	4.32.00	CDMA
Apple	iPad Pro	iOS 9.2.1 (13C75)	4.52.00	CDMA
LG	G5	Android 6.0.1	MMB29M	CDMA
Samsung	J3 – SM-J320V	Android 6.0.1	MMB29M.J320VVRU2AP12	CDMA
Google	Pixel XL	Android 7.1.1	NMF26U	CDMA
Samsung	GS7 – SM-G930V	Android 6.0.1	MMB29M.G930VVRU4AP13	CDMA
Samsung	GS7 Edge SM-G935V	Android 6.0.1	MMB29M.G935VVRS4APH1	CDMA
Motorola	Z Force XT1650	Android 7.0	NCLS25.86-11-4	CDMA
HTC 10	HTC6545LVW	Android 6.0.1	1.85.605.8.8.0_g CL774095	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

Katana Forensics Triage version 1.1802.220 was installed on Windows version 10.0.14393.

3.2 Internal Memory Data Objects

Katana Forensics Triage version 1.1802.220 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
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

Data Objects	Data Elements
Stand-alone data files	*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

Table 2: Internal Memory Data Objects

4 Test Results

This section provides the test cases results reported by the tool. Sections 4.1 – 4.2 identify the mobile device operating system type, media (e.g., Android, iOS) and the make and model of mobile devices used for testing Katana Forensics Triage version 1.1802.220.

The *Test Cases* column (internal memory acquisition) in sections 4.1 - 4.2 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 successfully.

Partial: the mobile forensic application returned some of 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 mobile forensic application is unable to perform the test or 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 and analyzed with Katana Forensics Triage version 1.1802.220.

All test cases pertaining to the acquisition of supported Android devices were successful with the exception of the following.

- When connectivity is disrupted during acquisition an error message is not returned for all Android devices.
- Subscriber and equipment related data (i.e., MSISDN, IMEI) was not reported for all Android devices.
- Graphic files associated with Contact/Address book entries are not reported for all Android devices.
- No Maps GPS related data (i.e., longitude, latitude) coordinates are reported for all Android devices.

See Table 3 below for more details.

Katana Forensics Triage version 1.1802.220

Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*						
		LG G5	Samsung J3	Google Pixel XL	Samsung GS7	Samsung GS7 Edge	Motorola Z Force	HTC 10
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Generated Reports	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Equipment/ User Data	IMEI	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
	MEID/ESN	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	MSISDN	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
PIM Data	Contacts	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
	Calendar	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Memos/ Notes	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Call Logs	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Missed	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
SMS Messages	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages	Graphic	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Audio	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Video	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application Data	Documents (txt, pdf files)	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Katana Forensics Triage version 1.1802.220								
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*						
		LG G5	Samsung J3	Google Pixel XL	Samsung GS7	Samsung GS7 Edge	Motorola Z Force	HTC 10
Social Media Data	Facebook	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Twitter	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	LinkedIn	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Instagram	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Internet Data	Bookmarks	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	History	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Email	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
GPS Data	Coordinates /Geo-tagged	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Non-Latin Character	Reported in native format	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Hashing	Case File/ Individual Files	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Case File Data Protection	Modify Case Data	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Table 3a: Android Mobile Devices

4.2 iOS Mobile Devices

The internal memory contents for iOS devices were acquired and analyzed with Katana Forensics Triage version 1.1802.220.

All test cases pertaining to the acquisition of supported iOS devices were successful with the exception of the following across all iOS devices.

- When connectivity is disrupted during acquisition an error message is not returned for all iOS devices.
- Graphic files associated with Contact/Address book entries are not reported for all iOS devices.
- The status of call logs (e.g., incoming, outgoing, missed) is not reported for the iPhone 5S.
- Notes/Memo entries are not reported for the iPhone 6S Plus, iPhone 7, iPhone 7 Plus, iPad Mini and iPad Pro.

See Table 4 below for more details.

Katana Forensics Triage version 1.1802.220							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone 5S	iPhone 6S Plus	iPhone 7	iPhone 7 Plus	iPad Mini	iPad Pro
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Generated Reports	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Equipment/ User Data	IMEI	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	MEID/ESN	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	MSISDN	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
PIM Data	Contacts	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
	Calendar	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Memos/Notes	*As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Call Logs	Incoming	*Partial*	*As Expected*	*As Expected*	*As Expected*	*NA*	*NA*
	Outgoing	*Partial*	*As Expected*	*As Expected*	*As Expected*	*NA*	*NA*
	Missed	*Partial*	*As Expected*	*As Expected*	*As Expected*	*NA*	*NA*
SMS Messages	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages	Graphic	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Audio	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Video	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Audio	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application Data	Documents (txt, pdf files)	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Social Media Data	Facebook	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*

Katana Forensics Triage version 1.1802.220							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone 5S	iPhone 6S Plus	iPhone 7	iPhone 7 Plus	iPad Mini	iPad Pro
Social Media Data	Twitter	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	LinkedIn	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Instagram	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Internet Data	Bookmarks	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	History	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Email	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
GPS Data	Coordinates/ Geo-tagged	*As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
Non-Latin Character	Reported in native format	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Hashing	Case File/ Individual Files	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Case File Data Protection	Modify Case Data	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Table 4: iOS Mobile Devices