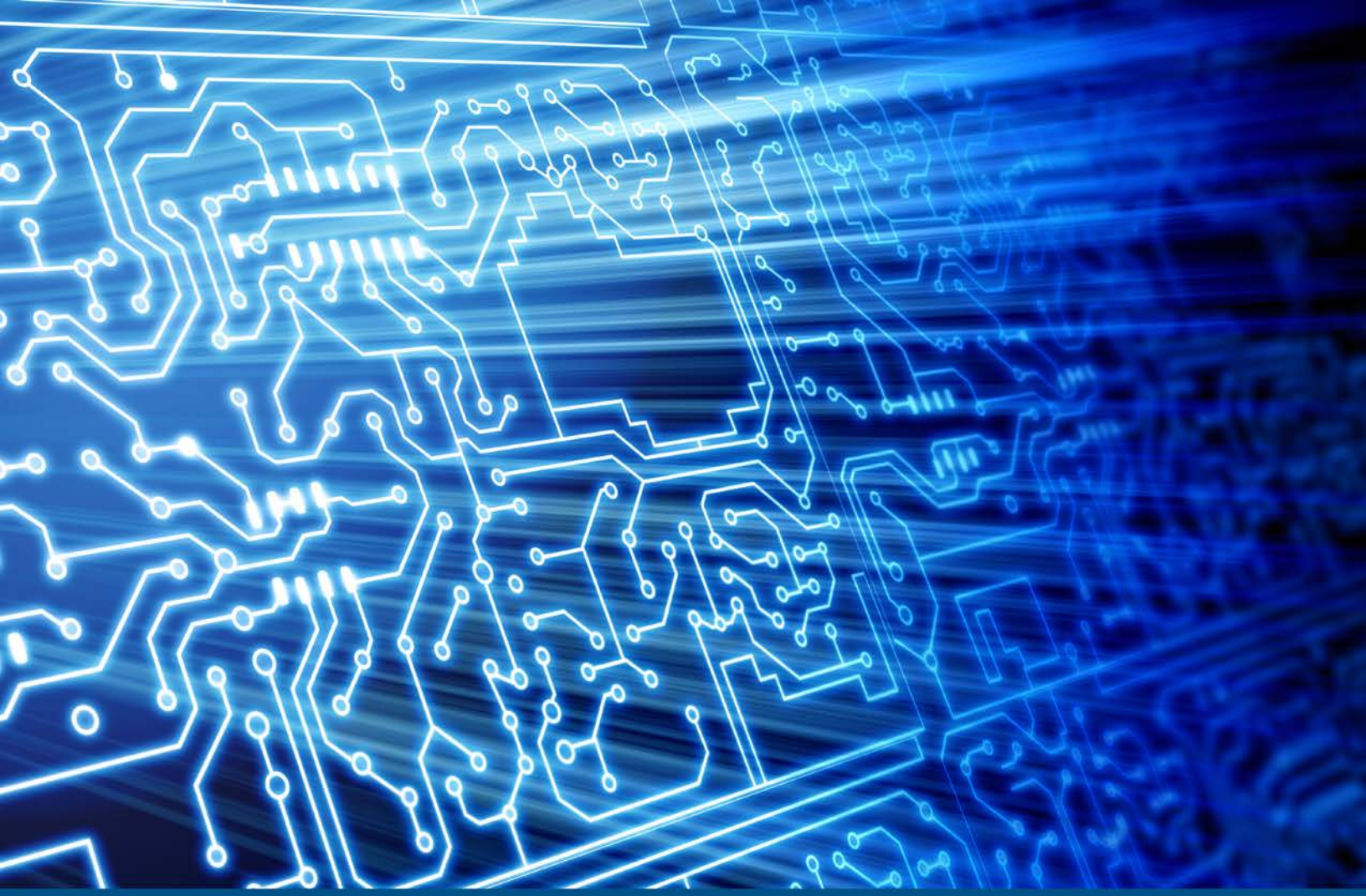

Device Seizure v6.8

Test Results for Mobile Device Acquisition Tool

June 22, 2015

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 www.cyber.st.dhs.gov**.**

June 2015

Test Results for Mobile Device Acquisition Tool:
Device Seizure v6.8

Contents

Introduction 3
How to Read This Report 3
1 Results Summary 2
2 Mobile Devices 4
3 Testing Environment 4
3.1 Execution Environment 5
3.2 Internal Memory Data Objects 5
3.3 UICC Data Objects 7
4 Test Results 7
4.1 Android Mobile Devices 8
4.2 iOS Mobile Devices 11
4.3 Feature Phones 13
4.4 Universal Integrated Circuit Cards (UICCs) 15

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 Device Seizure v6.8 across supported feature phones, Android and iOS devices. The images captured from the test runs are available at the CFReDS Web site (http://www.cfreds.nist.gov).

Test results from other tools can be found on the DHS S&T-sponsored digital forensics web page, http://www.cyberfetch.org/.

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 and Universal Integrated Circuit Cards (UICC) data objects used to populate the mobile devices and associated media. Section 4 provides an overview of the test case results reported by the tool. The full test data is available at http://www.cftt.nist.gov/mobile_devices.htm.

Test Results for Mobile Device Acquisition Tool

Tool Tested:	Device Seizure
Software Version:	v6.8
Supplier:	Paraben Corporation
Address:	21690 Red Rum Drive Ste 137 Ashburn, VA 20147
Tel:	(801) 796-0944
Email:	forensics@paraben.com
WWW:	http://www.paraben.com

1 Results Summary

Device Seizure is designed to perform a forensically sound extraction of data from a variety of mobile devices, such as feature phones, smart phones and other mobile devices.

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

***Presentation*:**

- Acquisition of internal memory of the phone and readability was not successful. (Devices: *Samsung Convoy3, LG Extravert*)

***Equipment / Subscriber related data*:**

- Subscriber related data (i.e., MSISDN) were not reported. (Devices: *Galaxy S3, Galaxy S4, HTC One GSM, iPhone 5 GSM and Nexus 4*)

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

- Acquisition of *calendar* entries was not successful. (Device: *HTC One GSM*)
- Acquisition of *memos* was not successful. (Device: *Galaxy S5, Galaxy Note 3, Nexus 4*)
- Acquisition of PIM data (i.e., *long memo*) was partially reported. (Devices: *iPhone 5S, iPad Mini CDMA, iPad CDMA, HTC One GSM, iPhone 5 GSM*).
- Acquisition of PIM data (i.e., *memos*) was partially reported. (Devices: *iPad Mini GSM, iPad GSM*).
- Acquisition of PIM data (i.e., *physical home address within a contact entry*) was not acquired. (Devices: *iOS devices*).
- Stand-alone audio files were not acquired. (Devices: *iPhone 5S, iPad Mini CDMA, iPad CDMA*)

Call Logs:

- Active incoming, outgoing and missed calls times and status flags were not acquired. (Device: *iPhone 5S*)

***SMS messages*:**

- Active SMS messages were not acquired. (Device: *iPad GSM*)

***MMS messages*:**

- Incoming and outgoing messages with video file attachments were not acquired. (Device: *iPhone 5S*)
- Active MMS messages were not acquired. (Devices: *iPad Mini GSM, iPad GSM*)

Internet Related Data:

- Browser History and Bookmarks were not acquired. (Device: *Galaxy Note3*)
- Browser History was not acquired. (Device: *iPad Mini GSM*)

Social Media Data:

- Acquisition of social media data (i.e., *Facebook, Twitter, LinkedIn*) was partial. (Devices: *Android devices, iOS devices*)

Case Data Protection:

- Partial notification of modified device memory data. (Devices: *Android devices, iOS devices*)

***GPS Related Data*:**

- Acquisition of longitude and latitude were not reported. (Devices: *Android devices*)

NOTES:

- Hash values for vendor supported data objects were reported only in the pdf report. This applies to all devices and UICCs.
- The purpose of DS hash validation is to prevent the usage of modified data from a device as evidence by detecting any third-party changes in acquired data. DS uses the following levels of acquired data protection:
  - All device data is encrypted.
  - DS calculates and stores hash values for each grid, file, and the entire case data.
  - To prevent modification of a file and its hash value, DS uses several interrelated levels for hash value calculation.

  If a modification of data with DS is done the case file will open but the data would not longer be available.

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing Device Seizure.

Make	Model	OS	Firmware	Network
Apple iPhone	5	iOS 6.1.4 (10B350)	3.04.25	GSM
Apple iPhone	5S	iOS 7.1 (11D167)	2.18.02	CDMA
Apple iPad	iPad 2 - MD065LL/A	iOS 6.1.3 (10B329)	04.12.05	GSM
Apple iPad	iPad Air - ME999LL/A	iOS 7.1 (11D167)	2.18.02	CDMA
Apple iPad Mini	iPad Mini - ME030LL/A	iOS 6.1.3 (10B329)	3.04.25	GSM
Apple iPad Mini	iPad Mini - MF075LL/A	iOS 7.0.4 (11B554a)	1.03.01	CDMA
Samsung Galaxy S3	SGH-1747	Android 4.1.2	1747UCDMG2	GSM
Samsung Galaxy S4	SGH-M919	Android 4.2.2	M919UVUAMDL	GSM
Samsung Galaxy S5	SM-G900V	Android 4.2.2	G900V.05	CDMA
HTC One	HTCC6525LVW	Android 4.2.2	0.89.20.0222	GSM
HTC One	HTC One	Android 4.1.2	4A.17.3250.20_10.40.1150.04L	CDMA
Samsung Galaxy Note 3	SM-N900V	Android 4.3	N900V.07	CDMA
Nexus 4	Nexus 4	Android 4.3	JWR66Y	GSM
Samsung	Convoy 3	Brew Mobile 1.0.4	U680.MJ2	CDMA
LG	Extravert	Brew Mobile 1.03	VN28010A	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 and UICCs.

3.1 Execution Environment

Device Seizure v6.8 was installed on Windows 7 v6.1.7601.

3.2 Internal Memory Data Objects

Device Seizure 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-ASCII Entry
PIM Data	
Datebook/Calendar	*Regular Length*
Memos	*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-ASCII SMS/EMS

Data Objects	Data Elements
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
Location Data	
	GPS Coordinates
Social Media Data	
	Facebook
	Twitter
	LinkedIn

Table 2: Internal Memory Data Objects

3.3 UICC Data Objects

The table below (Table 3) provides an overview of the data elements populated on Universal Integrated Circuit Cards (UICCs).

Data Objects	Data Elements
Abbreviated Dialing Numbers (ADN)	
	Maximum Length
	Special Character
	Blank Name
	Non-ASCII Entry
	Regular Length - Deleted Number
Call Logs	
	Last Numbers Dialed (LND)
Text Messages	
	Incoming SMS - Read
	Incoming SMS - Unread
	Non-ASCII SMS
	Incoming SMS - Deleted
	Non-ASCII EMS
	Incoming EMS - Deleted

Table 3: UICC 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 (e.g., Android, iOS) and the make and model of mobile devices used for testing Device Seizure v6.8. Section 4.4 covers Universal Integrated Circuit Cards (UICCs).

The *Test Cases* column (internal memory acquisition/UICC) in sections 4.1 - 4.4 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 and UICCs within each test case. Each individual sub-category row results for each mobile device/UICC 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 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 Device Seizure v6.8.

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

- Subscriber related data (i.e., MSISDN) were not reported for the Galaxy S3, Galaxy S4, HTC One GSM, and Nexus 4.
- Acquisition of PIM Data (i.e. *calendar entries*) was not reported for HTC One GSM.
- Acquisition of PIM Data (i.e. *memos*) was not reported for the Galaxy S5, Galaxy Note3 and Nexus 4.
- Acquisition of PIM Data (i.e. *long memos*) was partially reported for the HTC One GSM.
- Browser history and bookmarks for visited Internet URLs were not reported for the Samsung Galaxy Note 3.
- Social media data was partially acquired; only certain data from LinkedIn and Twitter was acquired for the Galaxy S5.
- Social media data was partially acquired; only certain data from LinkedIn, Facebook and Twitter was acquired for the Galaxy Note 3.
- Social media data was partially acquired; only certain data from Facebook was acquired for the Galaxy S3 and Galaxy S4.
- Social media data was partially acquired; only certain data from Twitter was acquired for the Nexus 4.
- Social media data was partially acquired; only the path to the installation package was recovered for the HTC One GSM.
- Partial notification of modified device memory data for all Android devices.
- GPS related data was not acquired for all Android devices.

NOTES:

- Deleted calendar entry was recovered for the Galaxy S4.
- Deleted memos were recovered for the Galaxy S3.
- Deleted SMS were recovered for the Galaxy S3 and Nexus 4.
- MMS status flags were incorrectly identified as “failed” when they had been successfully sent for the Galaxy S3 and Nexus 4.

See Table 4 below for more details.

Device Seizure v6.8							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*					
		Galaxy S3 *GSM*	Galaxy S4 *GSM*	Galaxy S5 *CDMA*	Galaxy Note 3 *CDMA*	HTC One *GSM*	Nexus 4 *GSM*
Connectivity	Non Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*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*	*NA*	*NA*	*As Expected*	*As Expected*
	MEID/ESN	*NA*	*NA*	*As Expected*	*As Expected*	*NA*	*NA*
	MSISDN	*Not As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*
PIM Data	Contacts	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Calendar	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*
	To-Do List/ Tasks	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Memos	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*Partial*	*Not As Expected*
Call Logs	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*
	Missed	*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*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages	Graphic	*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*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Device Seizure v6.8							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*					
		Galaxy S3 *GSM*	Galaxy S4 *GSM*	Galaxy S5 *CDMA*	Galaxy Note 3 *CDMA*	HTC One *GSM*	Nexus 4 *GSM*
Stand-alone Files	Graphic	*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*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application Data	Documents	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Spreadsheets	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Presentations	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Internet Data	Bookmarks	*As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	History	*As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
Social Media Data	Facebook	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*	*Not As Expected*
	Twitter	*Not As Expected*	*Not As Expected*	*Partial*	*Partial*	*Partial*	*Partial*
	LinkedIn	*Not As Expected*	*Not As Expected*	*Partial*	*Partial*	*Partial*	*Not As Expected*
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Selected All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Select Individual	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Case File Data Protection	Modify Case Data	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
Physical Acquisition	Readability	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Deleted File Recovery	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Non-ASCII Character	Reported in native format	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Hashing	Hashes reported for acquired data objects	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
GPS Data	Coordinates (Long/Lat)	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*

Table 4: Android Mobile Devices

4.2 iOS Mobile Devices

The internal memory contents for iOS devices were acquired and analyzed with Device Seizure v6.8.

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

- Subscriber related data (i.e., MSISDN) were not reported for the iPhone 5 GSM.
- Physical home address within a contact entry was not acquired for all iOS devices.
- Long memos were partially acquired for the iPhone 5S, iPad Mini CDMA, iPad CDMA and iPhone 5 GSM.
- Memos were partially acquired for the iPad GSM.
- Call logs times and status flags were not acquired for the iPhone 5S.
- MMS messages with video attachments were not acquired for the iPhone 5S.
- MMS messages were not acquired for the iPad Mini GSM and iPad GSM
- SMS messages were not acquired for the iPad GSM.
- Stand-alone audio files were not acquired for the iPhone 5S, iPad Mini CDMA and iPad CDMA.
- Internet related data (i.e., *browser history*) was not acquired for the iPad Mini GSM.
- Social media data was partially acquired; only certain data from LinkedIn and Facebook was acquired for the iPhone 5S.
- Social media data was partially acquired; only certain data from Twitter was acquired for the iPad Mini GSM.
- Social media data was partially acquired; only certain data from LinkedIn, Twitter and Facebook was acquired for the iPad GSM, iPhone 5 GSM, iPad Mini CDMA and iPad CDMA.
- Partial notification of modified device memory data for all iOS devices.

NOTES:

- Deleted contact entry was partially recovered for the iPhone 5S and iPad Mini CDMA.
- Deleted data (i.e., *calendar and contact entries, call logs, memos*) was recovered for the iPad Mini GSM.
- Status flags for missed calls were incorrectly identified as “failed incoming calls” for the iPhone 5 GSM.
- MMS attachments appear under the SMS messages category.
- Paths to social media data (i.e., *Facebook*) were recovered but not the data for the iPhone 5 GSM.

See Table 5 below for more details.

Device Seizure v6.8							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone 5 *GSM*	iPhone 5S *CDMA*	iPad *GSM*	iPad Air *CDMA*	iPad Mini *GSM*	iPad Mini *CDMA*
Connectivity	Non Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Generated Reports	*As Expected*	*Partial*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Equipment/ User Data	IMEI	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
	MEID/ESN	*NA*	*NA*	*NA*	*As Expected*	*NA*	*NA*
	MSISDN	*Not As Expected*	*As Expected*	*NA*	*NA*	*NA*	*NA*
PIM Data	Contacts	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
	Calendar	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	To-Do List/ Tasks	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Memos	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
Call Logs	Incoming	*As Expected*	*Partial*	*NA*	*NA*	*NA*	*NA*
	Outgoing	*As Expected*	*Partial*	*NA*	*NA*	*NA*	*NA*
	Missed	*As Expected*	*Partial*	*NA*	*NA*	*NA*	*NA*
SMS Messages	Incoming	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages	Graphic	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*
	Video	*As Expected*	*Not As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application	Documents	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Device Seizure v6.8							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone 5 *GSM*	iPhone 5S *CDMA*	iPad *GSM*	iPad Air *CDMA*	iPad Mini *GSM*	iPad Mini *CDMA*
Data	Spreadsheets	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Presentations	*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*	*Not As Expected*	*As Expected*
Social Media Data	Facebook	*Partial*	*Partial*	*Partial*	*Partial*	*Not As Expected*	*Partial*
	Twitter	*Partial*	*Not As Expected*	*Partial*	*Partial*	*Partial*	*Partial*
	LinkedIn	*Partial*	*Partial*	*Partial*	*Partial*	*Not As Expected*	*Partial*
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Selected All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Select Individual	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Case File Data Protection	Modify Case Data	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
Physical Acquisition	Readability	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Deleted File Recovery	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Non-ASCII Character	Reported in native format	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Hashing	Hashes reported for acquired data objects	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
GPS Data	Coordinates (Long/Lat)	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Table 5: iOS Mobile Devices

4.3 Feature Phones

The internal memory contents for the devices running Brew Mobile were acquired and analyzed with Device Seizure v6.8.

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

- Internal memory of the phone was not acquired; Therefore, readability of recovered data was not performed for the Samsung Convoy 3 CDMA or the LG Extravert CDMA.

NOTE:

- The tool is able to connect to the device but it is unable to acquire the data from it.

See Table 6 below for more details.

Device Seizure v6.8			
Test Cases – Internal Memory Acquisition		*Mobile Devices Platforms*	
		Brew Mobile	
		Samsung Convoy 3 *CDMA*	LG Extravert CDMA
Connectivity	Non Disrupted	*As Expected*	*As Expected*
	Disrupted	*As Expected*	*As Expected*
Reporting	Preview-Pane	*Not As Expected*	*Not As Expected*
	Generated Reports	*Not As Expected*	*Not As Expected*
Equipment/ User Data	IMEI	*NA*	*NA*
	MEID/ESN	*NA*	*NA*
	MSISDN	*NA*	*NA*
PIM Data	Contacts	*NA*	*NA*
	Calendar	*NA*	*NA*
	To-Do List/ Tasks	*NA*	*NA*
	Memos	*NA*	*NA*
Call Logs	Incoming	*NA*	*NA*
	Outgoing	*NA*	*NA*
	Missed	*NA*	*NA*
SMS	Incoming	*NA*	*NA*

Messages	Outgoing	*NA*	*NA*
MMS Messages	Graphic	*NA*	*NA*
	Audio	*NA*	*NA*
	Video	*NA*	*NA*
Stand-alone Files	Graphic	*NA*	*NA*
	Audio	*NA*	*NA*
	Video	*NA*	*NA*
Application Data	Documents	*NA*	*NA*
	Spreadsheets	*NA*	*NA*
	Presentations	*NA*	*NA*
Internet Data	Bookmarks	*NA*	*NA*
	History	*NA*	*NA*
Social Media Data	Facebook	*NA*	*NA*
	Twitter	*NA*	*NA*
	LinkedIn	*NA*	*NA*
Acquisition	Acquire All	*NA*	*NA*
	Selected All	*NA*	*NA*
	Select Individual	*NA*	*NA*
Case File Data Protection	Modify Case Data	*NA*	*NA*
Physical Acquisition	Readability	*NA*	*NA*
	Deleted File Recovery	*NA*	*NA*
Non-ASCII Character	Reported in native format	*NA*	*NA*
Hashing	Hashes reported for acquired data objects	*NA*	*NA*
GPS Data	Coordinates (Long/Lat)	*NA*	*NA*

Table 6: Feature Phones

4.4 Universal Integrated Circuit Cards (UICCs)

The internal memory contents for Universal Integrated Circuit Cards (UICCs) were acquired and analyzed with Device Seizure v6.8.

All test cases pertaining to the acquisition of UICCs were successful with the exception of the following:

- Notification of modified memory data was not successful for the UICCs.

NOTES:

- The counter for incorrect PIN/PUK attempts does not decrement on the first incorrect attempt.

See Table 7 below for more details.

Device Seizure v6.8		
Test Cases – UICC Acquisition		*Universal Integrated Circuit Card*
Connectivity	Non Disrupted	*As Expected*
	Disrupted	*As Expected*
Equipment/ User Data	Service Provider Name (SPN)	*As Expected*
	ICCID	*As Expected*
	IMSI	*As Expected*
	MSISDN	*As Expected*
PIM Data	Abbreviated Dialing Numbers (ADNs)	*As Expected*
	Last Numbers Dialed (LNDs)	*As Expected*
	SMS Messages	*As Expected*
	EMS Messages	*As Expected*
Location Related Data	LOCI	*As Expected*
	GPRSLOCI	*As Expected*
Acquisition	Acquire All	*As Expected*
	Selected All	*As Expected*
	Select Individual	*As Expected*
Case File Data Protection	Modify Case Data	*Not As Expected*
Password Protected SIM Acquire	Acquisition of Protected SIM	*As Expected*
PIN/PUK Attempts	PIN attempts reported	*As Expected*
	PUK attempts reported	*As Expected*
Non-ASCII Character	Non-ASCII characters	*As Expected*
Hashing	Hashes reported for acquired data objects	*As Expected*

Table 7: Universal Integrated Circuit Cards