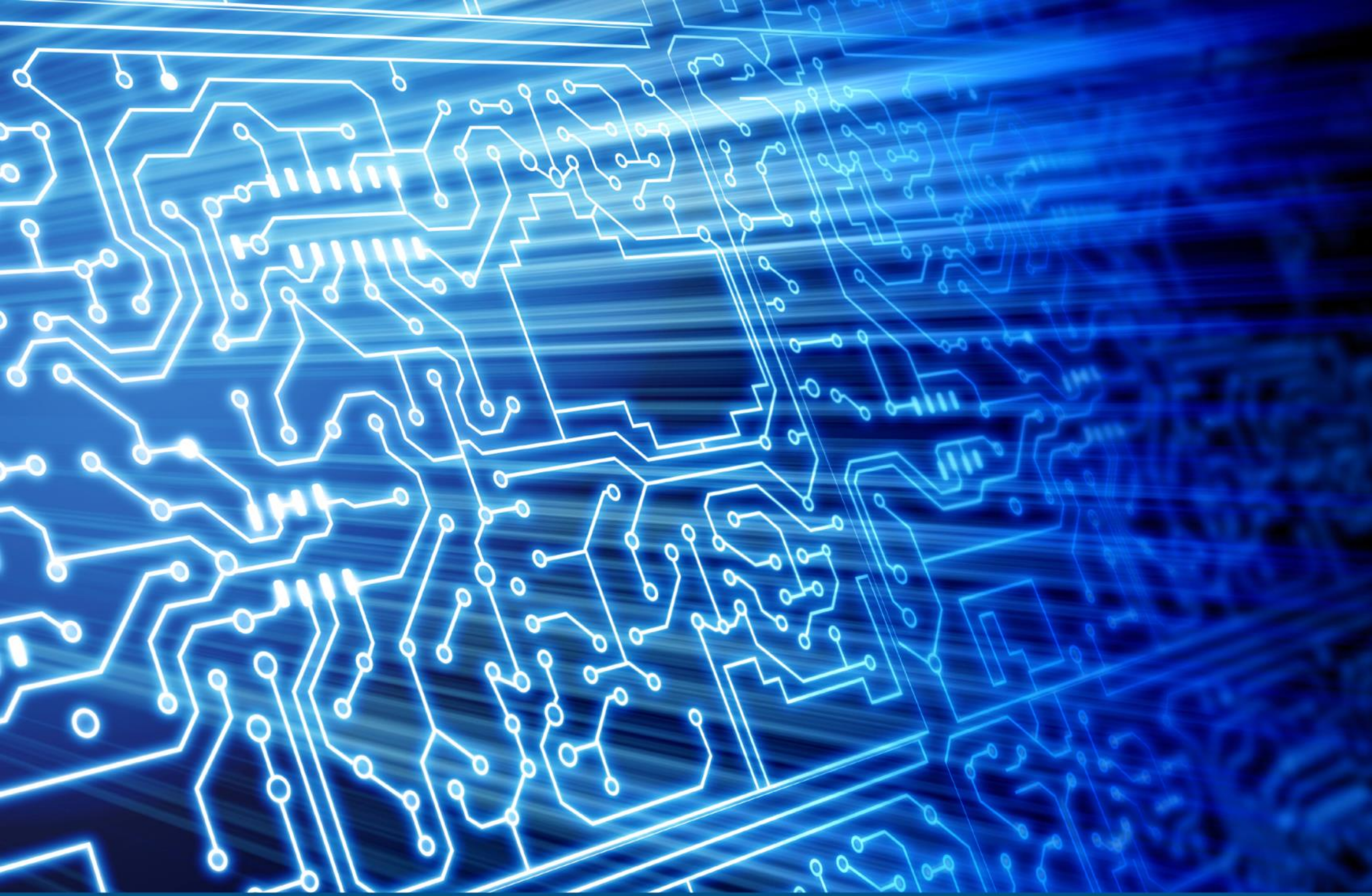

XRY v7.0.1.37853

Test Results for Mobile Device Acquisition Tool

November 30, 2016

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
DHS Science and Technology Cyber Security Division home page.

November 2016

Test Results for Mobile Device Acquisition Tool:
XRY v7.0.1.37853

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.

This document reports the results from testing XRY v7.0.1.37853 across supported mobile devices e.g., smart phones, feature phones.

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

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. The full test data is available at NIST's CFTT Mobile Devices home page.

Test Results for Mobile Device Acquisition Tool

Tool Tested:	XRY
Software Version:	v7.0.1.37853
Supplier:	Micro Systemation Inc
Address:	2001 Jefferson Davis Highway Suite 801 Arlington VA 22202
Tel:	(703) 750-0068
Fax:	(800) 371-9215
WWW:	Micro Systemation Inc. Web site

1 Results Summary

XRY v7.0.1.37853 is a software application designed to run on the Windows operating system, which allows you to perform a secure forensic extraction of data from a wide variety of mobile devices, such as smartphones, tablets, modems, music players and satellite navigation units. XRY supports thousands of different mobile devices and smartphone app versions.

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

Subscriber related Data:

- MSIDNs were not reported. (Devices: *BlackBerry Z10, BlackBerry Z30*)

Personal Information Management (PIM) Data:

- Contacts containing associated graphic files were not reported with the corresponding *contact*. The graphic files are reported separately within the `pimdata/graphics` folder. (Devices: *BlackBerry Z10, BlackBerry Z30*)
- Contacts containing metadata e.g., URLs, Addresses (city, state, zip) were not reported. (Devices: *BlackBerry Z10, BlackBerry Z30*)

Social media Data:

- Social media (Facebook, LinkedIn, Instagram) related data was not reported. (Device: *Galaxy S6*)
- Partial social media related data for Twitter (i.e., profile pics, pictures, emoticons) was reported. (Device: *Galaxy S6*)
- Social media (Facebook, Instagram) related data was not reported. (Devices: *iOS*)
- Partial social media related data for Twitter and LinkedIn (i.e., personal messages, graphics, profile information) was reported. (Devices: *iOS*)
- Social media (Facebook, LinkedIn, Twitter) related data was not reported. (Device: *BlackBerry Z30*)

- Partial social media related data for Facebook, Twitter and LinkedIn (i.e., profile pictures) were reported. (Devices: *BlackBerry Z10*)

Internet Related Data:

- Browser history, bookmarks and email related data were not reported. (Device: *Galaxy S6*)
- Browser history, bookmarks were not reported. (Device: *Samsung Rugby 3*)

GPS Related Data:

- GPS related – waypoints, routes, longitude and latitude coordinates were not acquired. (Devices: *Galaxy S6, Galaxy Tab-E, Galaxy Tab S2, Samsung Rugby III*)

NOTES:

- ► For all Android contact entries containing Chinese characters are incorrectly reported. The following contact: 阿恶哈拉 is reported twice but the order of the characters changes on the second iteration. For instance the second iteration characters 1-4 are reported in the following order: 3,4,1,2 resulting in: 阿恶哈拉 哈拉阿恶.
- ► For all Android devices supporting group messages – an individual message only containing contact data is reported in addition to group message.

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing XRY v7.0.1.37853.

Make	Model	OS	Firmware	Network
Apple iPhone	6	iOS 9.2.1 (13C75)	4.52.00	CDMA
Apple iPhone	6S	iOS 9.2.1 (13C75)	1.23.00	CDMA
Apple iPhone	6S Plus	iOS 9.2.1 (13C75)	1.23.00	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
Samsung Galaxy	S6	Android 5.1.1	LMY47.G920VVRU4BOK7	CDMA
Samsung Galaxy	Tab E	Android 5.1.1	LMY47X.T567VVRU1AOH1	CDMA
Samsung Galaxy	Tab S2	Android 5.1.1	LMY47X.T817BVRU2AOJ2	CDMA
Blackberry Z10	STL100-4	10 OS - 10.2.1.2122	672849	CDMA
Blackberry Z30	STA100-3	10 OS - 10.3.2.858	85718	CDMA
HTC Win 8x	HTC PM23300	Win 8.0	3030.0.34101.502	GSM
Samsung Rugby III	SGH-A997	A997UCM G1	REV0.2	GSM

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

XRY v7.0.1.37853 was installed on Windows 7 v6.1.7601.

3.2 Internal Memory Data Objects

XRY v7.0.1.37853 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	*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-Latin SMS/EMS
MMS Messages	
	Incoming Audio
	Incoming Graphic
	Incoming Video
	Outgoing Audio
	Outgoing Graphic
	Outgoing Video
Application Data	
	Device Specific App Data

Data Objects	Data Elements
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

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 (e.g., Android, iOS) and the make and model of mobile devices used for testing XRY v7.0.1.37853.

The *Test Cases* column (internal memory acquisition) in sections 4.1 - 4.3 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 with XRY v7.0.1.37853 and analyzed with XRY Reader v6.17.0.

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

- Partial social media related data for Twitter (i.e., profile pics, pictures, emoticons) were reported for the Galaxy S6. Profile data, personal messages and tweets were not reported.
- GPS (longitude / latitude coordinates) for map routes were not reported for all Android devices.

See Table 3 below for more details.

XRY v7.0.1.37853				
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*		
		Galaxy S6	Galaxy Tab-E	Galaxy Tab S2
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*As Expected*	*As Expected*	*As Expected*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*
	Generated Reports	*As Expected*	*As Expected*	*As Expected*
Equipment/ User Data	IMEI	*As Expected*	*As Expected*	*As Expected*
	MEID/ESN	*NA*	*NA*	*NA*
	MSISDN	*As Expected*	*As Expected*	*As Expected*
PIM Data	Contacts	*As Expected*	*As Expected*	*As Expected*
	Calendar	*As Expected*	*NA*	*NA*
	Memos/Notes	*NA*	*NA*	*NA*
Call Logs	Incoming	*As Expected*	*NA*	*NA*
	Outgoing	*As Expected*	*NA*	*NA*
	Missed	*As Expected*	*NA*	*NA*

XRY v7.0.1.37853				
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*		
		Galaxy S6	Galaxy Tab-E	Galaxy Tab S2
SMS Messages	Incoming	*As Expected*	*NA*	*NA*
	Outgoing	*As Expected*	*NA*	*NA*
MMS Messages	Graphic	*As Expected*	*NA*	*NA*
	Audio	*As Expected*	*NA*	*NA*
	Video	*As Expected*	*NA*	*NA*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*
Application Data	Documents (txt, pdf files)	*As Expected*	*NA*	*NA*
Social Media Data	Facebook	*Not As Expected*	*NA*	*NA*
	Twitter	*Partial*	*NA*	*NA*
	LinkedIn	*Not As Expected*	*NA*	*NA*
	Instagram	*Not As Expected*	*NA*	*NA*
Internet Data	Bookmarks	*Not As Expected*	*NA*	*NA*
	History	*Not As Expected*	*NA*	*NA*
	Email	*Not As Expected*	*NA*	*NA*
GPS Data	Coordinates/ Geo-tagged	*Not As Expected*	*Not As Expected*	*Not As Expected*
Non-Latin Character	Reported in native format	*As Expected*	*As Expected*	*As Expected*
Hashing	Case File/ Individual Files	*As Expected*	*As Expected*	*As Expected*
Case File Data Protection	Modify Case Data	*As Expected*	*As Expected*	*As Expected*

Table 3: Android Mobile Devices

4.2 iOS Mobile Devices

The internal memory contents for iOS devices were acquired with XRY v7.0.1.37853 and analyzed with XRY Reader v6.17.0.

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

- Social media related data i.e., profile information, status updates, personal messages, graphics were not reported for Facebook or Instagram for all iOS devices. Username, application files and application information are reported.
- Partial social medial related data i.e., personal messages, graphics, Username, application files and application information for Twitter and LinkedIn were reported for all iOS devices.

See Table 4 below for more details.

XRY v7.0.1.37853						
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*				
		iPhone 6	iPhone 6S	iPhone 6S Plus	iPad Mini	iPad Pro
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Generated Reports	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Equipment/ User Data	IMEI	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	MEID/ESN	*NA*	*NA*	*NA*	*NA*	*NA*
	MSISDN	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
PIM Data	Contacts	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Calendar	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Memos/Notes	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Call Logs	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Missed	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

XRY v7.0.1.37853						
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*				
		iPhone 6	iPhone 6S	iPhone 6S Plus	iPad Mini	iPad Pro
SMS Messages	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
MMS Messages	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application Data	Documents (txt, pdf files)	*NA*	*NA*	*NA*	*NA*	*NA*
Social Media Data	Facebook	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
	Twitter	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
	LinkedIn	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
	Instagram	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Internet Data	Bookmarks	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	History	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Email	*NA*	*NA*	*NA*	*NA*	*NA*
GPS Data	Coordinates/ Geo-tagged	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Non-Latin Character	Reported in native format	*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*
Case File Data Protection	Modify Case Data	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Table 4: iOS Mobile Devices

4.3 Blackberry / Windows / Feature Phones

The internal memory contents for the feature phone was acquired with XRY v7.0.1.37853 and analyzed with XRY Reader v6.17.0.

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

- Subscriber related data (i.e., MSISDN) was not reported for the BlackBerry Z10 or BlackBerry Z30.
- Contacts containing associated graphic files were not reported with the corresponding *contact* for the BlackBerry Z10 or the BlackBerry Z30.
- Contacts containing metadata e.g., URLs, Addresses (city, state, zip) were not reported for the BlackBerry Z10, BlackBerry Z30.
- Partial social media related data (i.e., profile pictures) were reported for the BlackBerry Z10
- Social media related data was not reported for the BlackBerry Z30.
- Internet related data (i.e., visited sites, bookmarks) are not reported for the Samsung Rugby 3.
- E-mail related data is not reported for the BlackBerry Z10 or the BlackBerry Z30.
- GPS related data is not reported for the Samsung Rugby 3.

NOTES:

- ► For the HTC Win 8x data extraction of only pictures and video is supported.
- ► For the Samsung Rugby 3 data extraction of call logs and email are not supported.

See Table 5 below for more details.

XRY v7.0.1.37853					
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Blackberry, Windows, Feature phones*			
		Blackberry Z10	Blackberry Z30	HTC Win 8x	Samsung Rugby 3
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Generated Reports	*As Expected*	*As Expected*	*As Expected*	*As Expected*

XRY v7.0.1.37853					
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Blackberry, Windows, Feature phones*			
		Blackberry Z10	Blackberry Z30	HTC Win 8x	Samsung Rugby 3
Equipment/ User Data	IMEI/IMSI	*As Expected*	*As Expected*	*NA*	*As Expected*
	MEID/ESN	*NA*	*NA*	*NA*	*NA*
	MSISDN	*Not As Expected*	*Not As Expected*	*NA*	*As Expected*
PIM Data	Contacts	*Partial*	*Partial*	*NA*	*As Expected*
	Calendar	*As Expected*	*As Expected*	*NA*	*As Expected*
	Memos/Notes	*NA*	*NA*	*NA*	*As Expected*
Call Logs	Incoming	*As Expected*	*As Expected*	*NA*	*NA*
	Outgoing	*As Expected*	*As Expected*	*NA*	*NA*
	Missed	*As Expected*	*As Expected*	*NA*	*NA*
SMS Messages	Incoming	*As Expected*	*As Expected*	*NA*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*NA*	*As Expected*
MMS Messages	Graphic	*As Expected*	*As Expected*	*NA*	*As Expected*
	Audio	*As Expected*	*As Expected*	*NA*	*As Expected*
	Video	*As Expected*	*As Expected*	*NA*	*As Expected*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*NA*	*As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application Data	Documents (txt, pdf files)	*As Expected*	*As Expected*	*NA*	*As Expected*
Social Media Data	Facebook	*Partial*	*Not As Expected*	*NA*	*NA*
	Twitter	*Partial*	*Not As Expected*	*NA*	*NA*
	LinkedIn	*Partial*	*Not As Expected*	*NA*	*NA*
	Instagram	*NA*	*NA*	*NA*	*NA*

XRY v7.0.1.37853					
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Blackberry, Windows, Feature phones*			
		Blackberry Z10	Blackberry Z30	HTC Win 8x	Samsung Rugby 3
Internet Data	Bookmarks	*NA*	*NA*	*NA*	*Not As Expected*
	History	*NA*	*NA*	*NA*	*Not As Expected*
	Email	*NA*	*NA*	*NA*	*NA*
GPS Data	Coordinates/ Geo-tagged	*NA*	*NA*	*NA*	*Not As Expected*
Non-Latin Character	Reported in native format	*As Expected*	*As Expected*	*NA*	*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*

Table 5: Feature Phones