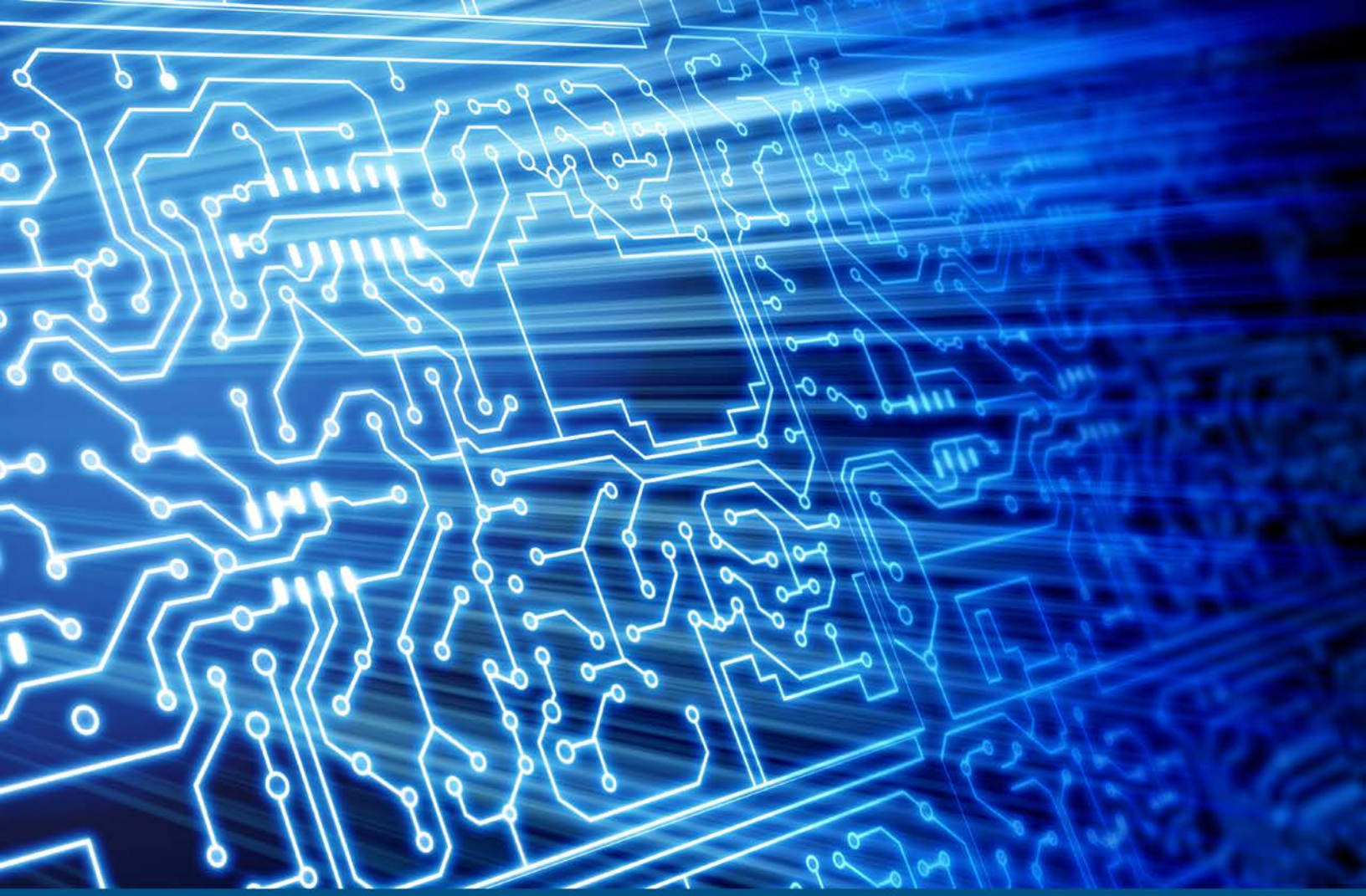

Oxygen Forensic Suite 2015 – Analyst v.7.0.0.408

Test Results for Mobile Device Acquisition Tool

March 27, 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**.**

March 2015

Test Results for Mobile Device Acquisition Tool:
Oxygen Forensic Suite 2015 - Analyst v7.0.0.408

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 Oxygen Forensic Suite 2015 – Analyst v7.0.0.408 across supported 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 and 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 http://www.cftt.nist.gov/mobile_devices.htm.

Test Results for Mobile Device Acquisition Tool

Tool Tested:	Oxygen Forensic Suite 2015 - Analyst
Software Version:	v7.0.0.408
Supplier:	Oxygen Forensics, Inc
Address:	901 N. Pitt St, Suite 320 Alexandria, VA 22314
Tel:	(877) 969-9436
Email:	mailto:support@oxygen-forensic.com
WWW:	http://www.oxygen-forensic.com/en/

1 Results Summary

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408 is mobile forensic software for data acquisition from phones, smartphones and other mobile devices.

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

***Connectivity*:**

- Connectivity for the following supported devices was not established. The drivers were installed and the OS recognized each device. (Devices: *Blackberry Q10, Blackberry Z10, Nexus* 4)
- Acquisition via advanced logical method was unsuccessful - the acquisition ran for 16 hours and hung on C:\FileRelay\MobileAsset\cpio.gz. (Device: *iPhone 5S CDMA)*

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

- Subscriber related data (i.e., MSISDN) was not reported. (Devices: *Android devices)*

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

- Contacts/address book entries were partially reported i.e., only the first and last word of the contact. (Devices: *Android devices)*
- Calendar entries were not reported under the "*Organizer"* category. (Devices: *Galaxy Note 3, HTC One GSM)*
- Memo/Note entries were not reported under the "*Organizer"* category. (Devices: *Android devices*)
- Acquisition of Call log data (i.e., incoming, outgoing, and missed calls) was not reported. (Devices: *Galaxy Note 3, HTC One GSM*)
- The status of deleted text messages were incorrectly reported as active. (Device: *Galaxy S5)*

- Recoverable deleted text messages were not reported. (Devices: *Galaxy S4, Galaxy Note 3, HTC One - CDMA and the HTC One - GSM*).

Internet Related Data:

- Bookmarks for visited Internet URLs were not reported under the category "*Web Browsers"*. (Device: *Galaxy Note 3, HTC One GSM*)

Social Media Related Data:

- Social media related data was partially acquired. (Device: *Galaxy S3, Galaxy S4, Galaxy S5, HTC One – GSM, iPad GSM, iPad CDMA, iPad Mini GSM, iPad Mini CDMA*)

***Case File Data Protection*:**

- Contents of the acquired data within a saved case file were modified for without warning. (Devices: *Samsung Galaxy S3, HTC One GSM and the HTC One CDMA*)
- Contents of the acquired data (via the Classic Logical method) within a saved case file were modified without warning. (Devices: *iPhone5S CDMA)*

GPS Related Data:

- GPS data i.e. longitude/latitude coordinates were not reported under the *"Application"* category – Navigation. (Device: *Galaxy S4*)

Note: After a successful acquisition of the HTC One (CDMA) the case file could not be saved to an assigned folder on the forensic workstation. The acquired device had to be opened for analysis then the case file had to be saved.

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing Oxygen Forensic Suite 2015 – Analyst v7.0.0.408.

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
Blackberry	Q10	BB 10.2.1.2122	672849	CDMA
Blackberry	Z10 – STL100-4	BB 10.2.1.2174	672849	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

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408 was installed on Windows 7 v6.1.7601.

3.2 Internal Memory Data Objects

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408 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

Data Objects	Data Elements
	Incoming EMS - Unread
	Outgoing EMS
	Incoming SMS - Deleted
	Outgoing SMS - Deleted
	Incoming EMS - Deleted
	Outgoing EMS - Deleted
	Non-ASCII 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
Location Data	
	GPS Coordinates
Social Media Data	
	Facebook
	Twitter
	LinkedIn

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 (i.e., Android, iOS) and the make and model of mobile devices used for testing Oxygen Forensic Suite 2015 – Analyst v7.0.0.408.

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 Oxygen Forensic Suite 2015 - Analyst v7.0.0.408.

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

- Connectivity was not established with the Nexus 4.
- Subscriber related data (i.e., MSISDN) were not acquired for all Android devices.
- Acquisition of PIM Data - *Contacts* were partially acquired (i.e., only the first and last name of the contact was reported for all Android devices.
- Acquisition of PIM Data – *Calendar* entries were not reported under the Oxygen's "Organizer" category for Galaxy Note3 and the HTC One GSM.
- Acquisition of PIM Data – *Memo/Notes* entries were not reported under the Oxygen's "Organizer" category for all Android devices.
- Acquisition of Call log data (i.e., incoming, outgoing, and missed calls) was not reported for the Galaxy Note 3 and the HTC One GSM.
- The status of deleted text messages were incorrectly reported as active for the Galaxy S5.
- Recoverable deleted text messages were not reported for the Galaxy S4, Galaxy Note 3, HTC One CDMA and the HTC One GSM.
- Bookmarks for visited Internet URLs were not reported under Oxygen's category "Web Browsers" for the Galaxy Note 3 and the HTC One GSM.
- Social media related data (Facebook, LinkedIn) was not acquired for the Galaxy S3, Galaxy S4, and the HTC One GSM.
- Social media related data (Facebook) was not acquired for the Galaxy S5.
- Contents of the acquired data within a saved case file were modified without warning for the Samsung Galaxy S3, HTC One GSM and the HTC One CDMA.
- GPS related data was not reported under "Application" category - Navigation for the Galaxy S4.

Note: After a successful acquisition of the HTC One CDMA the case file could not be saved to an assigned folder on the forensic workstation. The acquired device had to be opened for analysis then the case file had to be saved.

See Table 3 below for more details.

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408								
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*	HTC One *CDMA*	Nexus 4 *GSM*
Connectivity	Non Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*
	Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Generated Reports	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
Equipment/ User Data	IMEI	*As Expected*	*As Expected*	*NA*	*NA*	*As Expected*	*NA*	*NA*
	MEID/ESN	*NA*	*NA*	*As Expected*	*As Expected*	*NA*	*As Expected*	*NA*
	MSISDN	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*
PIM Data	Contacts	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*NA*
	Calendar	*As Expected*	*As Expected*	*As Expected*	*Partial*	*Partial*	*As Expected*	*NA*
	To-Do List/ Tasks	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Memos	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*NA*
Call Logs	Incoming	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*As Expected*	*NA*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*As Expected*	*NA*
	Missed	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*As Expected*	*NA*
SMS Messages	Incoming	*As Expected*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*NA*
	Outgoing	*As Expected*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*NA*
MMS Messages	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Video	*As*	*As*	*As*	*As*	*As*	*As*	*NA*

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408								
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*	HTC One *CDMA*	Nexus 4 *GSM*
		Expected	*Expected*	*Expected*	*Expected*	*Expected*	*Expected*	
Application Data	Documents	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Spreadsheets	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Presentations	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Internet Data	Bookmarks	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*As Expected*	*NA*
	History	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*As Expected*	*NA*
Social Media Data	Facebook	*Not As Expected*	*Not As Expected*	*Not As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*NA*
	Twitter	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	LinkedIn	*Not As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*NA*
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Selected All	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Select Individual	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Case File Data Protection	Modify Case Data	*Not As Expected*	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*NA*
Physical Acquisition	Readability	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Deleted File Recovery	*NA*	*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*	*NA*
Hashing	Hashes reported for acquired data objects	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
GPS Data	Coordinates (Long/Lat)	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*

Table 3: Android Mobile Devices

4.2 iOS Mobile Devices

The internal memory contents for iOS devices were acquired and analyzed with Oxygen Forensic Suite 2015 – Analyst v7.0.0.408.

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

- Acquisition via advanced logical method was unsuccessful for the iPhone5S CDMA. The acquisition ran for 16 hours and hung on C:\FileRelay\MobileAsset\cpio.gz. The Classic Logical method was utilized for testing.
- Contents of the acquired data (via the Classic Logical method) within a saved case file were modified for without warning for the iPhone5S.
- Social media data was partially acquired for the iPad GSM, iPad CDMA, iPad Mini GSM, iPad Mini CDMA devices.

Note: When running a previous version of iTunes 11.1 the following message occurs when attempting acquisition: Unlock the device to extract the data. Option 1 – Enter passcode on the device, Option 2 – Find lock down plist on PC to unlock the device.

See Table 4 below for more details.

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone5 *GSM*	iPhone5S *CDMA*	iPad *GSM*	iPad Air *CDMA*	iPad Mini *GSM*	iPad Mini *CDMA*
Connectivity	Non Disrupted	*As Expected*	*Partial*	*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*	*NA*	*As Expected*	*NA*	*As Expected*	*NA*
	MEID/ESN	*NA*	*As Expected*	*NA*	*As Expected*	*NA*	*As Expected*
	MSISDN	*As Expected*	*As Expected*	*NA*	*NA*	*NA*	*NA*
PIM Data	Contacts	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone5 *GSM*	iPhone5S *CDMA*	iPad *GSM*	iPad Air *CDMA*	iPad Mini *GSM*	iPad Mini *CDMA*
	Calendar	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	To-Do List/ Tasks	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Memos	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Call Logs	Incoming	*As Expected*	*As Expected*	*NA*	*NA*	*NA*	*NA*
	Outgoing	*As Expected*	*As Expected*	*NA*	*NA*	*NA*	*NA*
	Missed	*As Expected*	*As Expected*	*NA*	*NA*	*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	*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*
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*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	History	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Social Media Data	Facebook	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Twitter	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	LinkedIn	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Selected All	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*

Oxygen Forensic Suite 2015 – Analyst v7.0.0.408							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone5 *GSM*	iPhone5S *CDMA*	iPad *GSM*	iPad Air *CDMA*	iPad Mini *GSM*	iPad Mini *CDMA*
	Select Individual	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Case File Data Protection	Modify Case Data	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
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 4: iOS Mobile Devices