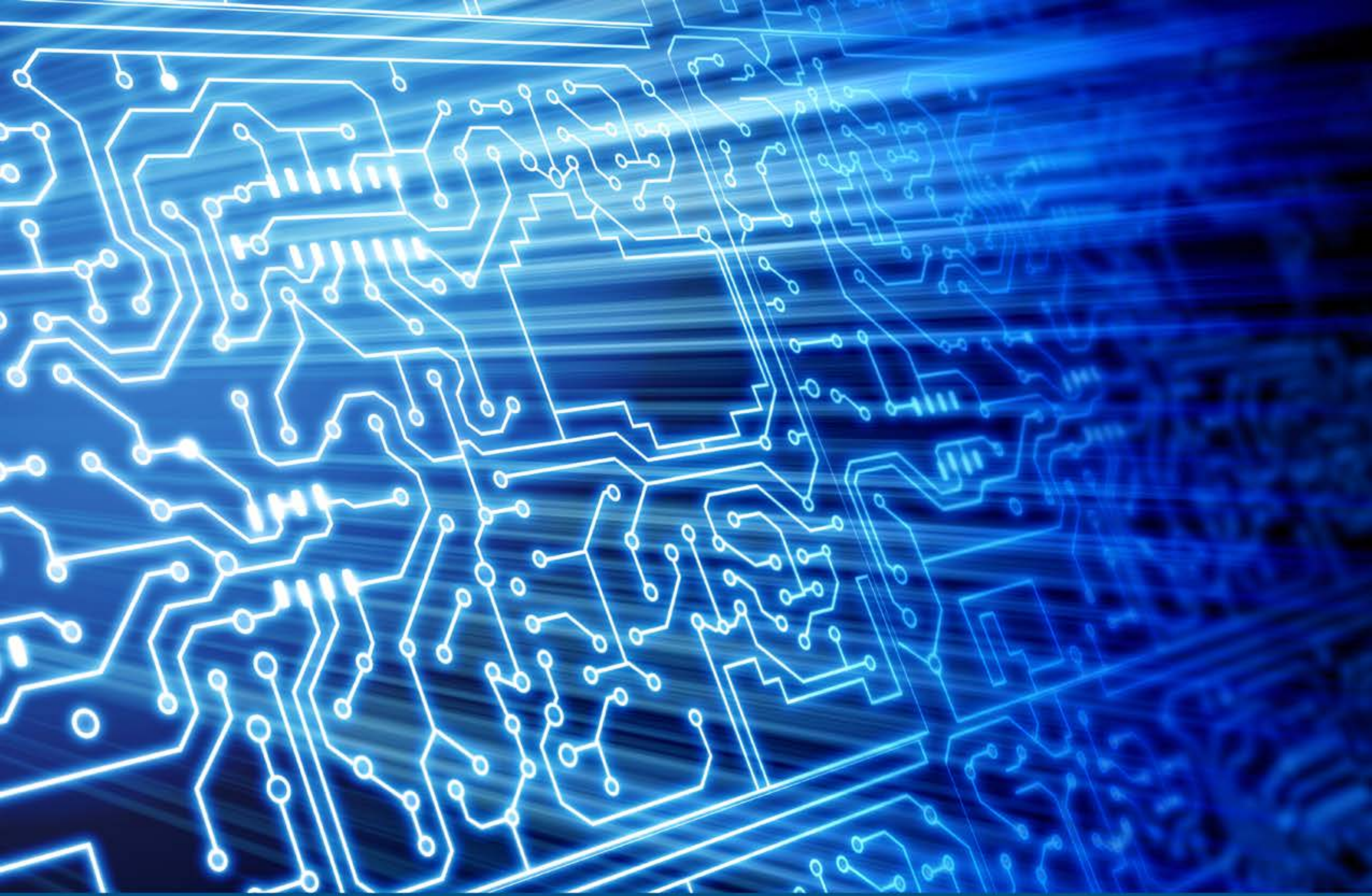

iOS Crime Lab v1.0.1

Test Results for Mobile Device Acquisition Tool

December 31, 2014

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.

December 2014

Test Results for Mobile Device Acquisition Tool:
iOS Crime Lab v1.0.1

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 Law Enforcement Standards Office (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation (FBI), 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 (ICE), U.S. Customs and Border Protection (CBP) and U.S. Secret Service (USSS). 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 iOS Crime Lab v1.0.1 across iOS mobile 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 site (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 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:	iOS Crime Lab
Software Version:	v1.0.1
Supplier:	Jonathan Zdziarski
WWW:	www.zdziarski.com

1 Results Summary

iOS Crime Lab is designed for data extractions from iOS mobile devices.

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

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing iOS Crime Lab.

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

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

iOS Crime Lab v1.0.1 was installed on Mac OS X v10.8.5.

3.2 Internal Memory Data Objects

iOS Crime Lab 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

Data Objects	Data Elements
	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
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

Data Objects	Data Elements
	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. Section 4.1 identifies the mobile device operating system type (i.e., iOS) and the make and model of mobile devices used for testing iOS Crime Lab v1.0.1.

The *Test Cases* column (internal memory acquisition) in section 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 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 iOS Mobile Devices

The internal memory contents for iOS devices were acquired with iOS Crime Lab v1.0.1.

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

See Table 3 below for more details.

iOS Crime Lab v1.0.1							
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*	*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	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Generated Reports	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
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*
	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*	*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*

iOS Crime Lab v1.0.1							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*					
		iPhone5 *GSM*	iPhone5S *CDMA*	iPad *GSM*	iPad Air *CDMA*	iPAD Mini *GSM*	iPad Mini *CDMA*
	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*	*As Expected*	*As Expected*	*As Expected*	*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*
	Select Individual	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Case File Data Protection	Modify Case Data	*As Expected*	*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 3: iOS Mobile Devices