BlackLight v2016.1

Test Results for Mobile Device Acquisition Tool

May 25, 2016

Homeland Security

Science and Technology

Test Results for Mobile Device Acquisition Tool:
BlackLight version 2016.1

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 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 (NIST CFTT).

This document reports the results from testing BlackLight v2016.1 across supported Android and iOS mobile devices.

Test results from other tools can be found on the DHS S&T web page, DHS Science and Technology Cyber Security Division.

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 CFTT Mobile Devices.

Test Results for Mobile Device Acquisition Tool

Tool Tested: BlackLight
Software Version: 2016.1

Supplier: BlackBag Technologies, Inc.

Address: 300 Piercy Road
                      San Jose, CA 95138 USA

Tel: (855) 844-8890
Email: support@blackbagtech.com
WWW: BlackBag Technologies

1   Results Summary

BlackLight 2016 release 1 is a comprehensive tool to help investigators conduct digital forensic investigations on Mac OS X computers, iOS devices (iPhone, iPad, iPod touch), Android devices, and Windows computers. The BlackLight graphical user interface was specifically designed to give forensics examiners both robust capabilities and an intuitive and elegant user experience throughout all phases of a digital forensic investigation.

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*:**
- Connectivity was not established. (Device: *Ellipsis 8*)
- Connectivity was established but generated errors. (Device: *iPhone 6S Plus*)

***Equipment / Subscriber related data*:**
- Subscriber related data (i.e., IMEI, MSISDN) was not reported. (Devices: *iPad Mini, iPad Pro*)

***Personal Information Management (PIM) data*:**
- Calendar and Notes entries are not reported in the user preview-pane under "Productivity". (Devices: *Motorola Droid Turbo 2, Galaxy S6, Galaxy S6 Edge Plus, LG G4, Galaxy Tab-E, Galaxy Tab S2*)
- Notes are not reported in the user preview-pane under "Productivity". Partial data can be found within notestore.sqlite. (Devices: *iPhone6, iPhone 6S, iPad Mini, iPad Pro*).
- Call logs are not reported. (Devices: *Galaxy Tab-E, Galaxy Tab S2*)
- Outgoing SMS Group messages are not reported. (Devices: *Motorola Droid Turbo 2, Galaxy S6, Galaxy S6 Edge Plus, LG G4*)
- SMS and MMS messages are not reported. (Devices: *Galaxy Tab-E, Galaxy Tab S2*)

- Incoming and outgoing deleted messages contain incorrect delivered and read dates. (Devices: *iPhone 6, iPhone 6S*)
- Active SMS messages have reported duplicates within the preview-pane with a deleted status. (Devices: *iPad Mini, iPad Pro*)
- MMS attachments (i.e., audio, graphic, video) are not viewable. (Devices: *Motorola Droid Turbo 2, Galaxy S6, Galaxy S6 Edge Plus, LG G4*)

Application Data:
- Application related data (i.e., txt, pdf files) was not acquired. (Devices: *iPhone 6, iPhone 6S, iPad Mini, iPad Pro*)

Stand-alone Files:
- Stand-alone video files contain incorrect creation and modified dates. (Devices: *iPhone 6, iPhone 6S, iPad Mini, iPad Pro*)

Social media Data:
- Social media related data is partially reported. (Devices: *Motorola Droid Turbo 2, Galaxy S6, Galaxy S6 Edge Plus, LG G4, Galaxy Tab-E, Galaxy Tab S2, iPhone 6, iPhone 6S, iPad Mini, iPad Pro*)

Internet Related Data:
- Browser history and bookmarks are not reported. (Devices: *Galaxy S6, Galaxy Tab-E, Galaxy Tab S2*)
- Email related data is not reported. (Devices: *Motorola Droid Turbo 2, Galaxy S6, Galaxy S6 Edge Plus, LG G4, Galaxy Tab-E, Galaxy Tab S2, iPhone 6, iPhone 6S, iPad Mini, iPad Pro*)

NOTES:
- Incoming and outgoing SMS/MMS messages are reported twice within the preview-pane. (Devices: *iPhone 6, iPhone 6S, iPad Mini, iPad Pro*).

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing BlackLight v2016.1.

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
Motorola Droid	Turbo2	Android 5.1.1	LCK23.130-23	CDMA
Samsung Galaxy	S6	Android 5.1.1	LMY47.G920VVRU4BOK7	CDMA
Samsung Galaxy	S6 Edge Plus	Android 5.1.1	LMY47X.G928VVRU2AOJ2	CDMA
LG	G4	Android 5.1.1	LMY47D	CDMA
Ellipsis	8	Android 4.4.2	QZ3_PE3X	CDMA
Samsung Galaxy	Tab E	Android 5.1.1	LMY47X.T567VVRU1AOH1	CDMA
Samsung Galaxy	Tab S2	Android 5.1.1	LMY47X.T817BVRU2AOJ2	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

BlackLight v2016.1 was installed on Windows 7 v6.1.7601.

3.2 Internal Memory Data Objects

BlackLight v2016.1 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
Stand-alone data files	

Data Objects	Data Elements
	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 – 4.2 identify the mobile device operating system type (e.g., Android, iOS) and the make and model of mobile devices used for testing BlackLight v2016.1.

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 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 BlackLight v2016.1.

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

- Connectivity to the Motorola Droid Turbo 2 (Android version 5.1.1, Build: LCK23.130-23) and the Ellipsis 8 (Android version 4.4.2, Build: KOT49H) were not established with BlackLight v2016.1.
- IMEI is not reported for the Galaxy S6, Galaxy S6 Edge Plus, LG G4, Galaxy Tab-E or the Galaxy Tab S2.
- Calendar and Notes are not reported in the "Productivity" tab for the Galaxy S6, Galaxy S6 Edge Plus, LG G4, Galaxy Tab-E or the Galaxy Tab S2.
- Call logs are not reported for the Galaxy Tab-E or the Galaxy Tab S2.
- Outgoing SMS Group messages are not reported for the Galaxy S6, Galaxy S6 Edge Plus or the LG G4
- SMS and MMS messages are not reported for the Galaxy Tab-E or the Galaxy Tab S2.
- MMS attachments (i.e., audio, graphic, video) are not viewable for the Galaxy S6, Galaxy S6 Edge Plus or the LG G4.
- Social media related data (e.g., profile information, status updates, pictures, video, and personal messages) are partially reported for the Galaxy S6, Galaxy S6 Edge Plus, LG G4, Galaxy Tab-E and the Galaxy Tab S2.
- Internet related data (i.e., history, bookmarks) are not reported for the Galaxy S6, Galaxy Tab-E or the Galaxy Tab S2.
- Email related data was not reported for the Galaxy S6, Galaxy S6 Edge Plus, LG G4, Galaxy Tab-E or the Galaxy Tab S2.

See Table 3 below for more details.

BlackLight version 2016 Release 1								
Test Cases – Internal Memory Acquisition		Mobile Device Platform: Android						
		Moto Droid Turbo 2	Galaxy S6	Galaxy S6 Edge Plus	LG G4	Ellipsis 8	Galaxy Tab-E	Galaxy Tab S2
Acquisition	Acquire All	As Expected	As Expected	As Expected	As Expected	Not As Expected	As Expected	As Expected
	Disrupted	As Expected	As Expected	As Expected	As Expected	NA	As Expected	As Expected
Reporting	Preview-Pane	As Expected	As Expected	As Expected	As Expected	NA	As Expected	As Expected
	Generated Reports	As Expected	As Expected	As Expected	As Expected	NA	As Expected	As Expected

BlackLight version 2016 Release 1							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*					
		Moto Droid Turbo 2	Galaxy S6	Galaxy S6 Edge Plus	LG G4	Ellipsis 8	Galaxy Tab-E	Galaxy Tab S2
Equipment/ User Data	IMEI	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
	MEID/ESN	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	MSISDN	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
PIM Data	Contacts	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
	Calendar	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*Not As Expected*	*Not As Expected*
	Memos/Notes	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*Not As Expected*	*Not As Expected*
Call Logs	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*Not As Expected*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*Not As Expected*
	Missed	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*Not As Expected*
SMS Messages	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*Not As Expected*
	Outgoing	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Not As Expected*	*Not As Expected*
MMS Messages	Graphic	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Not As Expected*	*Not As Expected*
	Audio	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Not As Expected*	*Not As Expected*
	Video	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Not As Expected*	*Not As Expected*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
Application Data	Documents (txt, pdf files)	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
Social Media Data	Facebook	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Partial*	*Partial*
	Twitter	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Partial*	*Partial*
	LinkedIn	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Partial*	*Partial*
	Instagram	*Partial*	*Partial*	*Partial*	*Partial*	*NA*	*Partial*	*Partial*

BlackLight version 2016 Release 1							
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: Android*					
		Moto Droid Turbo 2	Galaxy S6	Galaxy S6 Edge Plus	LG G4	Ellipsis 8	Galaxy Tab-E	Galaxy Tab S2
Internet Data	Bookmarks	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*Not As Expected*
	History	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*Not As Expected*
	Email	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*Not As Expected*	*Not As Expected*
GPS Data	Coordinates/ Geo-tagged	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
Non-Latin Character	Reported in native format	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
Hashing	Case File/ Individual Files	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
Case File Data Protection	Modify Case Data	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*

Table 3: Android Mobile Devices

4.2 iOS Mobile Devices

The internal memory contents for iOS devices were acquired and analyzed with BlackLight v2016.1.

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

- Connectivity to the iPhone 6S Plus (iOS 9.2.1 – 13C75) with BlackLight v2016.1 generated errors. The following error was reported, Errors: Unknown [Parse], BackupDir Empty [Parse], File Content Process cannot read file fork: 1[52]. Only stand-alone audio and graphic files were reported. The IMEI and the remaining defined data elements within table 2 were not reported.
- The IMEI and MSISDN are not reported for the iPad Mini or the iPad Pro.
- Notes are not reported in the "Productivity" tab for the iPhone 6, iPhone 6S, iPad Mini and iPad Pro. Partial notes data can be found in mobile/applications/com.apple.notes/notesstore.sqlite.
- Some incoming/outgoing deleted SMS messages contain incorrect dates, e.g., date delivered: 2001-01-01, 2026-01-18, 2062-10-29, date read: 2063-11-29 for the iPhone6 and iPhone 6s.

- Active messages for the iPad Mini and iPad Pro have reported duplicates with a deleted status.
- Mp4 files are reported with incorrect creation/modified dates as 1970-01-01 – should be 2016-02-09 for the iPhone 6, iPhone 6S, iPad Mini and the iPad Pro.
- Documents (txt, pdf files) are not reported for the iPhone 6, iPhone 6S, iPad Mini or the iPad Pro.
- Social media related data (e.g., profile information, status updates, pictures, video, and personal messages) are partially reported for the iPhone6, iPhone6S, iPad Mini and the iPad Pro.
- Email related data was not reported for the iPhone 6, iPhone 6S, iPad Mini or the iPad Pro.

NOTES:
- ➢ Blank name "Contacts/Address book" entries are acquired and reported, but may be overlooked within the preview-pane. The entry is obvious a record exists to examine – the entire line is blank.
- ➢ Notes are reported in the "Productivity" tab for earlier versions of iOS.
- ➢ Some incoming and outgoing SMS/MMS messages are reported twice for the iPhone 6, iPhone 6S, iPad Mini and iPad Pro.
- ➢ Some incoming and outgoing SMS/MMS messages are reported twice for the iPhone 6, iPhone 6S, iPad Mini and iPad Pro.
- ➢ The reported SMS messages within the "Communication" tab are not consistent with the Library/sms.db for the iPhone 6, iPhone 6S, iPad Mini and the iPad Pro.
- ➢ Music files are not reported within "Audio" tab – the following message is displayed: No Information Available. The files can be found: mobile/media/iTunes_Control/Music

See Table 4 below for more details.

BlackLight version 2016 Release 1					
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*	*Partial*	*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*

BlackLight version 2016 Release 1					
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*			
		iPhone 6	iPhone 6S	iPhone 6S Plus	iPad Mini	iPad Pro
Equipment/ User Data	IMEI	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
	MEID/ESN	*NA*	*NA*	*NA*	*NA*	*NA*
	MSISDN	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*
PIM Data	Contacts	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	Calendar	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	Memos/Notes	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*
Call Logs	Incoming	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	Missed	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
SMS Messages	Incoming	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*
	Outgoing	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*
MMS Messages	Graphic	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	Video	*As Expected*	*As Expected*	*Not 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	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*
Application Data	Documents (txt, pdf files)	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Social Media Data	Facebook	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*
	Twitter	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*
	LinkedIn	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*
	Instagram	*Partial*	*Partial*	*Not As Expected*	*Partial*	*Partial*

BlackLight version 2016 Release 1					
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*				
		iPhone 6	iPhone 6S	iPhone 6S Plus	iPad Mini	iPad Pro
Internet Data	Bookmarks	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	History	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
	Email	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
GPS Data	Coordinates/ Geo-tagged	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*	*As Expected*
Non-Latin Character	Reported in native format	*As Expected*	*As Expected*	*NA*	*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