Test Results for Binary Image (Joint Test Action Group (JTAG), Chip-Off) Decoding and Analysis Tool:
Cellebrite Universal Forensic Extraction Device (UFED) Physical Analyzer v7.20.0.123

January 2020

Homeland Security

Science and Technology

Test Results for Binary Image (Joint Test Action Group (JTAG), Chip-Off) Decoding and Analysis Tool:
Cellebrite Universal Forensic Extraction Device (UFED) Physical Analyzer v7.20.0.123

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security Science and Technology Directorate (DHS S&T), 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 Cellebrite's UFED Physical Analyzer (PA) v7.20.0.123 decoding and analysis of mobile devices JTAG and chip-off binaries.

Test results from other tools can be found on the DHS S&T-sponsored digital forensics web page, http://www.dhs.gov/science-and-technology/nist-cftt-reports.

Thanks, and appreciation to Rex Kiser and team from the Fort Worth Police Department – Digital Forensics Lab and Steve Watson and team from VTO Labs for their assistance on performing Chip-Off data extractions.

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.

Test Results for Binary Image (JTAG, Chip-Off) Decoding and Analysis Tool

Tool Tested:	Physical Analyzer
Software Version:	v7.20.0.123
Supplier:	Cellebrite, Inc.
Address:	7 Campus Drive, Suite 210 Parsippany, NJ 07054
Tel:	(415) 361-4077
Website:	http://www.cellebrite.com

1 Results Summary

Cellebrite's Physical Analyzer is a versatile mobile forensic solution that runs on existing hardware. It comes with a suite of applications, peripherals and accessories.

Physical Analyzer was tested for its ability to decode and analyze binary images created by performing Chip-Off and JTAG data extractions from supported mobile devices. Except for the following anomalies, the tool was able to decode and report all supported data objects completely and accurately for all mobile devices tested.

Stand-alone Files:
- Stand-alone files (i.e., audio, documents, graphics, video) are not reported. (Device: *HTC One Mini_Chip-off*)

Social Media Data:
- Social media related data (i.e., Twitter) is partially reported. (Devices: *LG K7_Chip-off, ZTE 970_Chip-off,*)
- Social media related data (i.e., Facebook) is partially reported. (Devices: *HTC One XL_Chip-off, HTC Desire S_Chip-off, HTC One XL_JTAG, HTC Desire S_JTAG*)

GPS-related Data:
- GPS related data (i.e., longitude, latitude coordinates, routes, addresses, etc.) was not reported. (Device: *HTC One Mini_Chip-off*)

For more test result details, see section 4.

2 Mobile Device Binary Images

The following table lists the mobile device binaries used for testing PA v7.20.0.123.

Make	Model	OS Version	Data Extraction
HTC	Desire 626	Android 5.1 Lollipop	Chip-Off
LG	K7	Android 5.1 Lollipop	Chip-Off
Samsung	S4	Android 4.2 Jelly Bean	Chip-Off, JTAG
ZTE	Z970	Android 4.4 KitKat	Chip-Off
HTC	Desire S	Android 2.3 Gingerbread	Chip-Off, JTAG
HTC	One XL	Android 4.0 Ice Cream Sandwich	Chip-Off, JTAG
HTC	One Mini	Android 4.2 Jelly Bean	Chip-Off, JTAG
Motorola	Moto-E	Android v5.1 Lollipop	Chip-Off
Samsung	S2	Android v2.3 Gingerbread	Chip-Off

Table 1: Mobile Device Binary Images

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

PA v7.20.0.123 was installed on Windows 10 Pro version 10.0.14393.

3.2 Internal Memory Data Objects

PA v7.20.0.123 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
Personal Information Manager (PIM) Data: Datebook/Calendar; Memos	*Regular Length*
	Maximum Length
	Deleted Entry
	Special Character
	Blank Entry
Call Logs	*Incoming*

Data Objects	Data Elements
Call Logs	*Outgoing*
	Missed
	Incoming – Deleted
	Outgoing – Deleted
	Missed - Deleted
Text Messages	*Incoming Short Message Service (SMS) – Read*
	Incoming SMS – Unread
	Outgoing SMS
	Incoming Enhanced Message Service (EMS) – Read
	Incoming EMS – Unread
	Outgoing EMS
	Incoming SMS – Deleted
	Outgoing SMS – Deleted
	Incoming EMS – Deleted
	Outgoing EMS – Deleted
	Non-Latin SMS/EMS
Multimedia Messaging Service (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
	E-mail
Location Data	*GPS Coordinates*
	Geo-tagged Data
Social Media Data	*Facebook*
	Twitter
	LinkedIn
	Instagram
	Pinterest
	Snapchat
	WhatsApp

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 make and model of the mobile device used for creating the binary image and data extraction technique employed (i.e.), Chip-Off, JTAG.

The *Test Cases* column in sections 4.1 and 4.2 are comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when decoding and analyzing the associated binary image. 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/ universal integrated circuit card (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 Chip-Off Data Extractions

The internal memory contents for Chip-Off binary images were decoded and analyzed with PA v7.20.0.123.

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

- Stand-alone files (i.e., audio, documents, graphics, video) were not reported for the HTC One Mini.
- Twitter social media data was partially reported i.e., account related information for the LG K7 and ZTE 970.
- Facebook social media data was partially reported i.e., account related information for the HTC One XL and HTC Desire S.
- GPS related data (e.g., waypoints, longitude, latitude, routes) were not reported for the HTC One Mini.

Notes:
-Devices defined in the table below with an '*' e.g., HTC One XL*, both Chip-Off and JTAG data extractions were performed.

-When performing the Chip-off data extraction, it appeared the HTC One Mini had suffered water damage, which may lead to differences in the data reported for the JTAG compared to Chip-off.

- ➢ Deleted Contacts, Calendar, Memo/Note entries were recovered for the HTC Desire 626, ZTE 970, Moto-E, Samsung S2, HTC One XL and Samsung S4.
- ➢ Deleted Contacts and Calendar entries were recovered for the LG K7 and HTC Desire S.
- ➢ Deleted Contac's and Memo entries were recovered for the HTC One Mini.
- ➢ Deleted Call logs were recovered for the LG K7, Moto-E, Samsung S2, Samsung S4 and HTC Desire S.
- ➢ Deleted SMS entries were recovered for the HTC Desire 626, LG K7, ZTE 970, Moto-E, Samsung S2, HTC One XL, Samsung S4, HTC One Mini and HTC Desire S.
- ➢ Deleted bookmark entries were recovered for the HTC Desire 626, ZTE 970, Moto-E, Samsung S2, HTC One XL, and HTC Desire S.

See Table 3 below for more details.

PA v7.20.0.123									
Test Cases – Chip-Off Binary Decoding and Analysis		*Mobile Device Binary Images: Chip-Off*								
		HTC Desire 626	LG K7	ZTE 970	Moto-E	Samsung S2	HTC One XL*	Samsung S4*	HTC One Mini*	HTC Desire S*
Equipment/ User Data	International Mobile Equipment Identity (IMEI)	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	MEID/ Electronic Serial Number (ESN)	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Mobile Station International Subscriber Directory Number (MSISDN	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
PIM Data	Contacts	*As Expected*	*As Expected*	*As Expected*	*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*	*As Expected*	*As Expected*	*As Expected*
	Memos/ Notes	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*
Call Logs	Incoming	*As Expected*	*As Expected*	*As Expected*	*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*	*As Expected*	*As Expected*	*As Expected*
	Missed	*As Expected*	*As Expected*	*As Expected*	*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*	*As Expected*	*As Expected*	*As Expected*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*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*	*As Expected*	*As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*As Expected*	*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*	*As Expected*	*As Expected*	*As Expected*
Stand-alone Files	Graphic	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*
	Audio	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*As Expected*

Test Cases – Chip-Off Binary Decoding and Analysis		Mobile Device Binary Images: Chip-Off								
		HTC Desire 626	LG K7	ZTE 970	Moto-E	Samsung S2	HTC One XL*	Samsung S4*	HTC One Mini*	HTC Desire S*
Application Data	Documents (txt, pdf files)	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	Not As Expected	As Expected
Social Media Data	Facebook	As Expected	As Expected	As Expected	As Expected	As Expected	Partial	As Expected	As Expected	Partial
	Twitter	As Expected	Partial	Partial	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	LinkedIn	As Expected	As Expected	NA	As Expected	NA	NA	NA	NA	NA
	Instagram	As Expected	As Expected	As Expected	As Expected	As Expected	NA	As Expected	NA	NA
	Pinterest	NA	As Expected	As Expected	NA	NA	NA	As Expected	NA	NA
	Snapchat	NA	As Expected	As Expected	NA	NA	NA	As Expected	NA	NA
	WhatsApp	NA	As Expected	As Expected	NA	NA	NA	NA	NA	NA
Internet Data	Bookmarks	As Expected	As Expected	As Expected	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	As Expected	As Expected	As Expected
	Email	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
GPS Data	Coordinates/ Geo-tagged	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	Not As Expected	As Expected
Non-Latin Character	Reported in native format	As Expected	As Expected	As Expected	As Expected	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	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	As Expected	As Expected	As Expected	As Expected

Table 3: Chip-Off Data Extractions

4.2 JTAG Data Extractions

The internal memory contents for JTAG binary images were decoded and analyzed with PA v7.20.0.123.

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

- Facebook social media data was partially reported (i.e., account information) for the HTC Desire S and HTC One XL.

Notes:
-Devices defined in the table below with an '' e.g., HTC One Mini*, both Chip-Off and JTAG data extractions were performed.*

- ➢ Deleted Contacts and Calendar entries were recovered for the HTC Desire S.
- ➢ Deleted Contacts and Memo/Note entries were recovered for the HTC One Mini.
- ➢ Deleted Contacts, Calendar and Memo/Note entries were recovered for the HTC One XL and Samsung S4.
- ➢ Deleted Call logs were recovered for the HTC Desire S and Samsung S4.
- ➢ Deleted SMS entries were recovered for the HTC Desire S, HTC One Mini, HTC One XL and Samsung S4.
- ➢ Deleted bookmark entries were recovered for the HTC Desire S, HTC One XL and Samsung S4.

See Table 4 below for more details.

PA v7.20.0.123				
Test Cases – JTAG Binary Decoding and Analysis	*Mobile Device Binary Images: JTAG*			
	HTC Desire S*	HTC One Mini*	HTC One XL*	Samsung S4*
Equipment/ User Data — IMEI	As Expected	As Expected	As Expected	As Expected
Equipment/ User Data — MEID/ESN	*NA*	*NA*	*NA*	*NA*
Equipment/ User Data — MSISDN	As Expected	As Expected	As Expected	As Expected
PIM Data — Contacts	As Expected	As Expected	As Expected	As Expected
PIM Data — Calendar	As Expected	As Expected	As Expected	As Expected
PIM Data — Memos/Notes	As Expected	As Expected	As Expected	As Expected
Call Logs — Incoming	As Expected	As Expected	As Expected	As Expected
Call Logs — Outgoing	As Expected	As Expected	As Expected	As Expected
Call Logs — Missed	As Expected	As Expected	As Expected	As Expected
SMS Messages — Incoming	As Expected	As Expected	As Expected	As Expected
SMS Messages — Outgoing	As Expected	As Expected	As Expected	As Expected
MMS Messages — Graphic	As Expected	As Expected	As Expected	As Expected
MMS Messages — Audio	As Expected	As Expected	As Expected	As Expected
MMS Messages — Video	As Expected	As Expected	As Expected	As Expected
Stand-alone Files — Graphic	As Expected	As Expected	As Expected	As Expected
Stand-alone Files — Audio	As Expected	As Expected	As Expected	As Expected
Stand-alone Files — Video	As Expected	As Expected	As Expected	As Expected
Application Data — Documents (txt, pdf files)	As Expected	As Expected	As Expected	As Expected
Social Media Data — Facebook	*Partial*	As Expected	*Partial*	As Expected
Social Media Data — Twitter	As Expected	As Expected	As Expected	As Expected
Social Media Data — LinkedIn	*NA*	*NA*	*NA*	*NA*
Social Media Data — Instagram	*NA*	*NA*	*NA*	As Expected

PA v7.20.0.123				
Test Cases – JTAG Binary Decoding and Analysis	_Mobile Device Binary Images: JTAG_			
	HTC Desire S*	_HTC One Mini*_	_HTC One XL*_	_Samsung S4*_
Social Media Data — Pinterest	_NA_	_NA_	_NA_	_As Expected_
Social Media Data — Snapchat	_NA_	_NA_	_NA_	_As Expected_
Social Media Data — WhatsApp	_NA_	_NA_	_NA_	_NA_
Internet Data — Bookmarks	_As Expected_	_As Expected_	_As Expected_	_As Expected_
Internet Data — History	_As Expected_	_As Expected_	_As Expected_	_As Expected_
Internet Data — Email	_As Expected_	_As Expected_	_As Expected_	_As Expected_
GPS Data — Coordinates/ Geo-tagged	_As Expected_	_Not As Expected_	_As Expected_	_As Expected_
Non-Latin Character — Reported in native format	_As Expected_	_As Expected_	_As Expected_	_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 4: JTAG Data Extractions