



Test Results for Binary Image (JTAG, Chip-Off) Decoding and Analysis Tool:
Paraben's Electronic Evidence Examiner – Device Seizure (E3:DS)
v2.3.12037.16428

September 27, 2019



**Homeland
Security**

Science and Technology

This report was prepared for the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) by the Office of Law Enforcement Standards of the National Institute of Standards and Technology.

For additional information about ongoing DHS S&T cybersecurity projects, please visit <https://www.dhs.gov/science-and-technology/cyber-security-division>.

September 2019

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

Paraben's Electronic Evidence Examiner – Device Seizure (E3:DS)
v2.3.12037.16428

Contents

Introduction	1
How to Read This Report	1
1 Results Summary	2
2 Mobile Device Binary Images	4
3 Testing Environment.....	4
3.1 Execution Environment	4
3.2 Internal Memory Data Objects.....	4
4 Test Results	6
4.1 Chip-Off Data Extractions	7
4.2 JTAG Data Extractions	10

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.cfft.nist.gov/>).

This document reports the results from testing Paraben's E3:DS v2.3.12037.16428 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-cfft-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:	Paraben's E3:DS
Software Version:	V2.3.12037.16248
Supplier:	Paraben
Address:	39344 John Mosby Hwy Ste 277 Aldie VA 20105-2000
Tel:	(801) 796-0944
WWW:	http://www.paraben.com

1 Results Summary

Paraben's E3:DS is a stand-alone mobile device data extraction and analysis solution that supports a large variety of mobile device types containing over 26,000+ device profiles. E3:DS supports data extraction for all smartphone operating systems, a variety of feature phones, tablets, GPS, PDAs and UICCs.

E3:DS 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 acquired all supported data objects completely and accurately for all mobile devices tested.

Subscriber and Equipment Related Data:

- Subscriber and equipment related data had to be manually located. The search facility did not return a positive hit. (Devices: *HTC Desire S_Chip-off*, *HTC Desire S_JTAG*)

Personal Information Management (PIM) Data:

- Contacts are partially reported within the Contacts2.db-wal file. (Devices: *Samsung S4_Chip-off*, *Samsung S4_JTAG*, *HTC Desire S_Chip-off*, *HTC Desire S_JTAG*)
- Calendar entries are partially reported within the Calendar.db-wal file. (Devices: *HTC Desire S_Chip-off*, *HTC Desire S_JTAG*)
- Memos/Notes are not reported. (Device: *HTC One Mini_Chip-off*)

Call Log Data:

- Call logs are not reported. (Devices: *HTC Desire S_Chip-off*, *HTC Desire S_JTAG*)

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., Facebook) is partially reported. (Devices: *HTC Desire 626_Chip-off*, *HTC One XL_Chip-off*, *HTC One XL_JTAG*)
- Social media related data (i.e., Facebook) is not reported. (Devices: *HTC Desire S_Chip-off*, *HTC Desire S_JTAG*)
- Social media related data (i.e., Twitter, Snapchat, WhatsApp) is partially reported. (Devices: *LG K7_Chip-off*, *ZTE 970_Chip-off*)

GPS Related Data:

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

For more test result details see section 4.

2 Mobile Device Binary Images

The following table lists the mobile device binaries used for testing E3:DS v2.3.12037.16248.

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

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

E3:DS v2.3.12037.16428 was installed on Windows 10 Pro version 10.0.14393.

3.2 Internal Memory Data Objects

E3:DS v2.3.12037.16428 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	<i>Regular Length</i>
	<i>Maximum Length</i>
	<i>Special Character</i>
	<i>Blank Name</i>
	<i>Regular Length, email</i>
	<i>Regular Length, graphic</i>
	<i>Regular Length, Address</i>
	<i>Deleted Entry</i>
	<i>Non-Latin Entry</i>
PIM Data: Datebook/Calendar; Memos	<i>Contact Groups</i>
	<i>Regular Length</i>
	<i>Maximum Length</i>
	<i>Deleted Entry</i>
	<i>Special Character</i>
	<i>Blank Entry</i>

Data Objects	Data Elements
Call Logs	<i>Incoming</i>
	<i>Outgoing</i>
	<i>Missed</i>
	<i>Incoming – Deleted</i>
	<i>Outgoing – Deleted</i>
	<i>Missed - Deleted</i>
Text Messages	<i>Incoming SMS – Read</i>
	<i>Incoming SMS – Unread</i>
	<i>Outgoing SMS</i>
	<i>Incoming EMS – Read</i>
	<i>Incoming EMS – Unread</i>
	<i>Outgoing EMS</i>
	<i>Incoming SMS – Deleted</i>
	<i>Outgoing SMS – Deleted</i>
	<i>Incoming EMS – Deleted</i>
	<i>Outgoing EMS – Deleted</i>
	<i>Non-Latin SMS/EMS</i>
MMS Messages	<i>Incoming Audio</i>
	<i>Incoming Graphic</i>
	<i>Incoming Video</i>
	<i>Outgoing Audio</i>
	<i>Outgoing Graphic</i>
	<i>Outgoing Video</i>
Application Data	<i>Device Specific App Data</i>
Stand-alone data files	<i>Audio</i>
	<i>Graphic</i>
	<i>Video</i>
	<i>Audio – Deleted</i>
	<i>Graphic - Deleted</i>
	<i>Video - Deleted</i>
Internet Data	<i>Visited Sites</i>
	<i>Bookmarks</i>
	<i>E-mail</i>
Location Data	<i>GPS Coordinates</i>
	<i>Geo-tagged Data</i>
Social Media Data	<i>Facebook</i>
	<i>Twitter</i>
	<i>LinkedIn</i>
	<i>Instagram</i>
	<i>Pinterest</i>
	<i>SnapChat</i>
	<i>WhatsApp</i>

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/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 E3:DS v2.3.12037.16428.

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

- Subscriber and equipment related data had to be manually located for the HTC Desire S. There were no positive search hits returned.
- Contacts are partially reported in the Contacts2.db-wal file for the Samsung S4.
- Contacts and calendar entries are partially reported in the Contacts2.db-wal and Calendar.db-wal files for the HTC Desire S.
- Memos/Notes were not reported for the HTC One Mini.
- Call Logs were not reported for the HTC Desire S.
- Stand-alone files (i.e., audio, documents, graphics, video) were not reported for the HTC One Mini.
- Facebook social media data was partially reported i.e., account related information for the HTC Desire 626 and HTC One XL.
- Facebook social media data was not reported for the HTC Desire S.
- Twitter, Snapchat and WhatsApp data were partially reported i.e., account related information for the LG K7 and ZTE 970.
- 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 Contact entries were recovered for the HTC Desire 626, LG K7, ZTE 970, HTC One XL, Samsung S4, HTC One Mini and HTC Desire S.
- Deleted Calendar entries were recovered for the HTC Desire 626, LG K7, ZTE 970, HTC One XL, Samsung S4 and HTC Desire S.
- Deleted Memo/Note entries were recovered for the HTC Desire 626 and HTC One XL.
- Deleted SMS entries were recovered for the HTC Desire 626, LG K7, ZTE 970, HTC One XL, Samsung S4, HTC One Mini and HTC Desire S.

See Table 3 below for more details.

E3:DS v2.3.12037.16428

E3:DS v2.3.12037.16428								
Test Cases – Chip-Off Binary Decoding and Analysis		Mobile Device Binary Images: Chip-Off						
		HTC Desire 626	LG K7	ZTE 970	HTC One XL*	Samsung S4*	HTC One Mini*	HTC Desire S*
Equipment/ User Data	IMEI	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	Partial
	MEID/ESN	NA	NA	NA	NA	NA	NA	NA
	MSISDN	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	Partial
PIM Data	Contacts	As Expected	As Expected	As Expected	As Expected	Partial	As Expected	Partial
	Calendar	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	Partial
	Memos/ Notes	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	Not As Expected
	Outgoing	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	Not As Expected
	Missed	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	Not As Expected
SMS Messages	Incoming	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
MMS Messages	Graphic	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
	Video	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	Not As Expected	As Expected
	Audio	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	Not As Expected	As Expected
Application Data	Documents (txt, pdf files)	As Expected	As Expected	As Expected	As Expected	As Expected	Not As Expected	As Expected
Social Media Data	Facebook	Partial	As Expected	As Expected	Partial	As Expected	As Expected	Not As Expected
	Twitter	As Expected	Partial	Partial	As Expected	As Expected	As Expected	As Expected
	LinkedIn	As Expected	As Expected	NA	NA	NA	NA	NA

E3:DS v2.3.12037.16428								
Test Cases – Chip-Off Binary Decoding and Analysis		Mobile Device Binary Images: Chip-Off						
		HTC Desire 626	LG K7	ZTE 970	HTC One XL*	Samsung S4*	HTC One Mini*	HTC Desire S*
Social Media Data	Instagram	As Expected	As Expected	As Expected	NA	As Expected	NA	NA
	Pinterest	NA	As Expected	As Expected	NA	As Expected	NA	NA
	SnapChat	NA	Partial	Partial	NA	As Expected	NA	NA
	WhatsApp	NA	Partial	Partial	NA	NA	NA	NA
Internet Data	Bookmarks	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
	Email	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	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
Hashing	Case File/ Individual Files	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

Table 3: Chip-Off Data Extractions

4.2 JTAG Data Extractions

The internal memory contents for JTAG binary images were decoded and analyzed with E3:DS v2.3.12037.16428.

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

- Subscriber and equipment related data had to be manually located for the HTC Desire S. There were no positive search hits returned.
- Contacts and calendar entries are partially reported in the Contacts2.db-wal and Calendar.db-wal files for the HTC Desire S.
- Contacts are partially reported in the Contacts2.db-wal file for the Samsung S4.
- Call Logs were not reported for the HTC Desire S.
- Facebook social media data is not reported for the HTC Desire S.
- Facebook social media data was partially reported (i.e., account information) for the HTC One XL.
- 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 Desire S*, both Chip-Off and JTAG data extractions were performed.*

- Deleted Contact and Calendar entries were recovered for the HTC Desire S, HTC One XL and Samsung S4.
- Deleted Memo/Note entries were recovered for the HTC One XL.
- Deleted SMS entries were recovered for the HTC Desire S, HTC One Mini, HTC One XL and Samsung S4.

See Table 4 below for more details.

E3:DS v2.3.12037.16428					
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	Partial	As Expected	As Expected	As Expected
	MEID/ESN	NA	NA	NA	NA
	MSISDN	Partial	As Expected	As Expected	As Expected
PIM Data	Contacts	Partial	As Expected	As Expected	Partial
	Calendar	Partial	As Expected	As Expected	As Expected
	Memos/Notes	As Expected	As Expected	As Expected	As Expected
Call Logs	Incoming	Not As Expected	As Expected	As Expected	As Expected
	Outgoing	Not As Expected	As Expected	As Expected	As Expected
	Missed	Not As Expected	As Expected	As Expected	As Expected
SMS Messages	Incoming	As Expected	As Expected	As Expected	As Expected
	Outgoing	As Expected	As Expected	As Expected	As Expected
MMS Messages	Graphic	As Expected	As Expected	As Expected	As Expected
	Audio	As Expected	As Expected	As Expected	As Expected
	Video	As Expected	As Expected	As Expected	As Expected
Stand-alone Files	Graphic	As Expected	As Expected	As Expected	As Expected
	Audio	As Expected	As Expected	As Expected	As Expected
	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	Not As Expected	As Expected	Partial	As Expected
	Twitter	As Expected	As Expected	As Expected	As Expected
	LinkedIn	NA	NA	NA	NA
	Instagram	NA	NA	NA	As Expected

E3:DS v2.3.12037.16428					
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
	SnapChat	NA	NA	NA	As Expected
	WhatsApp	NA	NA	NA	NA
Internet Data	Bookmarks	As Expected	As Expected	As Expected	As Expected
	History	As Expected	As Expected	As Expected	As Expected
	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