



Axiom v3.9.0.18130

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

March 2020



**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/cybersecurity> .

March 2020

**Test Results for Binary Image Joint Test Action Group (JTAG),
(Chip- Off) Decoding and Analysis Tool: Axiom v3.9.0.18130**

Contents

Introduction	1
How to Read This Report	1
1 Results Summary	2
2 Mobile Device Binary Images	2
3 Testing Environment	3
3.1 Execution Environment	3
3.2 Internal Memory Data Objects	3
4 Test Results	5
4.1 Chip-Off Data Extractions	6
4.2 JTAG Data Extractions	9

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology Special Program Office and Information Technology Laboratory. 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 DHS 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 Website (<https://www.cftt.nist.gov/>).

This document reports the results from testing Axiom v3.9.0.18130 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 webpage, <https://www.dhs.gov/science-and-technology/nist-cftt-reports>.

Thanks and appreciation to Rex Kiser and his team from the Fort Worth Police Department – Digital Forensics Lab and Steve Watson and his 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: Axiom

Software Version: v3.9.0.18130

Supplier: Magnet Forensics

Address: 2250 Corporate Park Drive, Suite 130
Herndon, VA 20171

Phone: 1-844-638-7884

Website: magnetforensics.com

1 Results Summary

Below is a comprehensive summary of how Axiom v3.9.0 performed when parsing and extracting supported data objects and elements from the JTAG and Chip-Off images of mobile devices. Except for the following anomalies, the tool was able to decode and report all supported data objects completely and accurately for all Chip-Off and JTAG binary images tested.

Social Media Data:

- Twitter social media data was partially reported i.e., account related information. (Device: *LG K7_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 Axiom v3.9.0.

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

Axiom v3.9.0 was installed on Windows 10 Pro version 10.0.14393.

3.2 Internal Memory Data Objects

Axiom v3.9.0 was tested for its ability to parse and extract supported data objects and elements from the JTAG and Chip-Off images of the test mobile devices. Table 2 below, defines the data objects and elements used for populating the 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>
	<i>Contact Groups</i>
Personal Information Manager (PIM) Data: Datebook/Calendar; Memos	<i>Regular Length</i>
	<i>Maximum Length</i>
	<i>Deleted Entry</i>
	<i>Special Character</i>
	<i>Blank Entry</i>
Call Logs	<i>Incoming</i>
	<i>Outgoing</i>
	<i>Missed</i>
	<i>Incoming – Deleted</i>
	<i>Outgoing – Deleted</i>
	<i>Missed – Deleted</i>

Table 2: Internal Memory Data Objects

Data Objects	Data Elements
Text Messages	<i>Incoming Short Message Service (SMS) – Read</i>
	<i>Incoming SMS – Unread</i>
	<i>Outgoing SMS</i>
	<i>Incoming Enhanced Message Service (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>
Multimedia Messaging Service (MMS) Messages	<i>Incoming Audio</i>
	<i>Incoming Graphic</i>
	<i>Incoming Video</i>
	<i>Outgoing Audio</i>
	<i>Outgoing Graphic</i>
Application Data	<i>Outgoing Video</i>
	<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>
Internet Data	<i>Video – Deleted</i>
	<i>Visited Sites</i>
	<i>Bookmarks</i>
Location Data	<i>E-mail</i>
	<i>GPS Coordinates</i>
Social Media Data	<i>Geo-tagged Data</i>
	<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 (Continued)

4 Test Results

This section provides the test case 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 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 parsed and extracted supported data objects from the JTAG, Chip-Off binary successfully.

Partial: the mobile forensic application returned some of data from the JTAG, Chip-Off binary.

Not As Expected: the mobile forensic application failed to return expected test results – the tool did not acquire or report supported data from the JTAG, Chip-Off binary 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 Axiom v3.9.0.

All test cases pertaining to the acquisition of supported Android devices were successful except for the following:

- Twitter social media data was partially reported i.e., account related information. (Device: LG K7)

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, Samsung S2, HTC One XL, Samsung S4, and HTC One Mini.
- Deleted Contacts and Calendar entries were recovered for the LG K7 and HTC Desire S.
- Deleted Call logs were recovered for the LG K7, ZTE 970, Samsung S2, HTC One XL, Samsung S4, HTC One Mini, and HTC Desire S.
- Deleted SMS entries were recovered for the HTC Desire 626, LG K7, ZTE 970, 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, Samsung S2, HTC One XL, Samsung S4, HTC One Mini, and HTC Desire S.

See Table 3 below for more details.

Axiom v3.9.0									
Test Cases – Chip-Off Binary Decoding and Analysis		Mobile Device Binary Images: Chip-Off							
		HTC Desire 626	LG K7	ZTE 970	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
	Mobile Equipment Identity (MEID)/Electronic Serial Number (ESN)	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
PIM Data	Contacts	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
	Memos/Notes	As Expected	As Expected	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	As Expected	As Expected
	Outgoing	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
SMS Messages	Incoming	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
MMS Messages	Graphic	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
	Video	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected

Table 3: Chip-Off Data Extractions

Axiom v3.9.0									
Test Cases – Chip-Off Binary Decoding and Analysis		Mobile Device Binary Images: Chip-Off							
		HTC Desire 626	LG K7	ZTE 970	Samsung S2	HTC One XL*	Samsung S4*	HTC One Mini*	HTC Desire S*
Stand-Alone Files	Graphic	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	NA	NA
	Audio	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	NA	NA
	Video	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	NA	NA
Application Data	Documents (txt, pdf files)	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Social Media Data	Facebook	As Expected	As Expected	As Expected	As Expected	NA	As Expected	As Expected	NA
	Twitter	As Expected	Partial	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	LinkedIn	As Expected	As Expected	NA	NA	NA	NA	NA	NA
	Instagram	As Expected	As Expected	As Expected	As Expected	NA	As Expected	NA	NA
	Pinterest	NA	As Expected	As Expected	NA	NA	As Expected	NA	NA
	SnapChat	NA	As Expected	As Expected	NA	NA	As Expected	NA	NA
	WhatsApp	NA	As Expected	As Expected	NA	NA	NA	NA	NA
Internet Data	Bookmarks	As Expected	NA	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	History	As Expected	NA	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
GPS Data	Coordinates/Geo-tagged	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
Hashing	Case File/Individual Files	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

Table 3: Chip-Off Data Extractions (Continued)

4.2 JTAG Data Extractions

The internal memory contents for JTAG binary images were decoded and analyzed with Axiom v3.9.0.

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

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

See Table 4 below for more details.

Axiom v3.9.0					
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
	MEID/ESN	NA	NA	NA	NA
	MSISDN	As Expected	As Expected	As Expected	As Expected
PIM Data	Contacts	As Expected	As Expected	As Expected	As Expected
	Calendar	As Expected	As Expected	As Expected	As Expected
	Memos/Notes	As Expected	As Expected	As Expected	As Expected
Call Logs	Incoming	As Expected	As Expected	As Expected	As Expected
	Outgoing	As Expected	As Expected	As Expected	As Expected
	Missed	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	NA	As Expected	NA	As Expected
	Twitter	As Expected	As Expected	As Expected	As Expected
	LinkedIn	NA	NA	NA	NA
	Instagram	NA	NA	NA	As Expected

Axiom v3.9.0					
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	NA	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