Test Results for Mobile Device Acquisition Tool:
Elcomsoft v8.30/AXIOM v7.7.0.38007

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology's (NIST) Special Programs 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's Criminal Investigation Division Electronic Crimes Program, and U.S. 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 Elcomsoft v8.30/AXIOM v7.7.0.83007 across supported mobile devices e.g., smart phones, tablets.

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

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 Mobile Device Acquisition Tool

Tool Tested: iOS Forensic Toolkit v8.30

Supplier: Elcomsoft Co. Ltd.

Address: Československé armády 371/11,
Praha 6-Bubeneč,
Czech Republic, PSČ 160 00

WWW: https://www.elcomsoft.com/

1   Results Summary

Elcomsoft v8.30/AXIOM v7.7.0.83007 was tested for its ability to acquire active data from the internal memory of supported mobile devices (i.e., smart phones).

The data reported for the devices below varies based upon the data extraction technique supported. For instance, a physical and/or file system extraction will provide the user with more data than a logical extraction. Each supported data extraction technique was performed. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

Social Media Data:
- Social media related data (LinkedIn, Pinterest) is partially reported. (Devices: ***all iOS***)
- Social media related data (TikTok) is partially reported. (Device: ***iPhone 11***)
- Social media related data (Facebook, Twitter/X, Snapchat, TikTok) is not reported. (Devices: ***all iOS***)

NOTE:

All acquisition options supported for each device was attempted. However, only logical acquisition finished successfully for all devices.

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing Elcomsoft v8.30/AXIOM v7.7.0.83007.

Make	Model	OS	Firmware or Serial Number	Network
Apple iPhone	8	iOS 11.3.1 (15E302)	1.89.00	CDMA
Apple iPhone	SE	iOS 15.1 (MX9N2LL/A)	1.06.00	CDMA
Apple iPhone	XR	iOS 15.1	7.02.00	CDMA
Apple iPhone	11	iOS 15.1 (15E302)	3.0.00	CDMA
Apple iPhone	13	iOS 15.6	MM9V61W17K	CDMA
Apple iPhone	13 Mini	iOS 15.6	M2NJF9FKVN	CDMA
Apple iPhone	13 Pro	iOS 15.6	FQ9K7W024F	CDMA
Apple iPhone	13 Pro Max	iOS 15.6	LR6H5XW3RP	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

Elcomsoft v8.30/AXIOM v7.7.0.83007 was installed on Windows 10 Pro for Workstation version 10.0.19042.

3.2 Internal Memory Data Objects

Elcomsoft v8.30/AXIOM v7.7.0.83007 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*

Data Objects	Data Elements
PIM Data: Datebook/Calendar; Memos	*Regular Length* *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	*Audio* *Graphic* *Video* *Audio – Deleted* *Graphic – Deleted* *Video – Deleted*
Internet Data	*Visited Sites* *Bookmarks* *E-mail*
Location Data	*GPS Coordinates* *Geo-tagged Data*

Data Objects	Data Elements
Social Media Data	*Facebook*
	Twitter/X
	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. Section 4.1 identifies the mobile device operating system type (iOS) and the make and model of mobile devices used for testing Elcomsoft v8.30/AXIOM v7.7.0.83007.

The *Test Cases* column (internal memory acquisition) in section 4.1 is 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 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 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 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 and analyzed with Elcomsoft v8.30/AXIOM v7.7.0.83007.

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

- Social media related data (LinkedIn, Pinterest) is partially reported for all iOS.
- Social media related data (TikTok) is partially reported for the iPhone 11.
- Social media related data (Facebook, Twitter/X, Snapchat, TikTok) for all iOS.

See Tables 3a, 3b below for more details.

Mobile Device Platform: iOS

Test Cases:	iPhone 8	iPhone SE	iPhone XR	iPhone 11	iPhone 13	iPhone 13 Mini
Acquisition: Acquire All	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Acquisition: Disrupted	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Reporting: Preview-Pane	NA	NA	NA	NA	NA	NA
Reporting: Generated Reports	NA	NA	NA	NA	NA	NA
Equipment/User Data: IMEI/MEID/ESN	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Equipment/User Data: MSISDN	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
PIM Data: Calendar	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
PIM Data: Memos/Notes	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Call Logs: Incoming	As Expected	As Expected	NA	As Expected	As Expected	As Expected
Call Logs: Outgoing	As Expected	As Expected	NA	As Expected	As Expected	As Expected
Call Logs: Missed	As Expected	As Expected	NA	As Expected	As Expected	As Expected
SMS Messages: Incoming	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
SMS Messages: 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
MMS Messages: Audio	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
MMS Messages: 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
Stand-alone Files: Audio	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Stand-alone Files: Video	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Application Data: Documents (txt, pdf files)	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Social Media Data: Facebook	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected	Not As Expected

Test Cases:	iPhone 8	iPhone SE	iPhone XR	iPhone 11	iPhone 13	iPhone 13 Mini
Social Media Data: Twitter/X	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Social Media Data: LinkedIn	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Social Media Data: Instagram	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Social Media Data: Pinterest	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Social Media Data: SnapChat	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
Social Media Data: WhatsApp	*Not As Expected*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
Social Media Data: TikTok	*NA*	*NA*	*NA*	*Not As Expected*	*NA*	*NA*
Internet Data: Bookmarks	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Internet Data: History	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Internet Data: Email	*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*
Non-Latin Character: Reported in native format	*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*
Case File Data Protection: Modify Case Data	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
SQLite Data: Report Active Data	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
SQLite Data: Run SQLite Commands	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*

Table 3a: iOS Devices

Internal Memory Acquisition
Elcomsoft v8.30
Mobile Device Platform: iOS

Test Cases:	iPhone 13 Pro	iPhone 13 Pro Max
Acquisition: Acquire All	*As Expected*	*As Expected*
Acquisition: Disrupted	*As Expected*	*As Expected*
Reporting: Preview-Pane	*NA*	*NA*
Reporting: Generated Reports	*NA*	*NA*
Equipment/User Data: IMEI/MEID/ESN	*As Expected*	*As Expected*
Equipment/User Data: MSISDN	*As Expected*	*As Expected*
PIM Data: Contacts	*As Expected*	*As Expected*
PIM Data: Calendar	*As Expected*	*As Expected*
PIM Data: Memos/Notes	*As Expected*	*As Expected*
Call Logs: Incoming	*As Expected*	*As Expected*
Call Logs: Outgoing	*As Expected*	*As Expected*
Call Logs: Missed	*As Expected*	*As Expected*
SMS Messages: Incoming	*As Expected*	*As Expected*
SMS Messages: Outgoing	*As Expected*	*As Expected*
MMS Messages: Graphic	*As Expected*	*As Expected*
MMS Messages: Audio	*As Expected*	*As Expected*
MMS Messages: Video	*As Expected*	*As Expected*
Stand-alone Files: Graphic	*As Expected*	*As Expected*
Stand-alone Files: Audio	*As Expected*	*As Expected*
Stand-alone Files: Video	*Not As Expected*	*As Expected*
Application Data: Documents (txt, pdf files)	*As Expected*	*As Expected*
Social Media Data: Facebook	*Not As Expected*	*Not As Expected*

Test Cases:	iPhone 13 Pro	iPhone 13 Pro Max
Social Media Data: Twitter/X	*Not As Expected*	*Not As Expected*
Social Media Data: LinkedIn	*Not As Expected*	*Not As Expected*
Social Media Data: Instagram	*Not As Expected*	*Not As Expected*
Social Media Data: Pinterest	*Not As Expected*	*Not As Expected*
Social Media Data: SnapChat	*Not As Expected*	*Not As Expected*
Social Media Data: WhatsApp	*Partial*	*Partial*
Social Media Data: TikTok	*NA*	*NA*
Internet Data: Bookmarks	*As Expected*	*As Expected*
Internet Data: History	*As Expected*	*As Expected*
Internet Data: Email	*As Expected*	*As Expected*
GPS Data: Coordinates/Geo-tagged	*As Expected*	*As Expected*
Non-Latin Character: Reported in native format	*As Expected*	*As Expected*
Hashing: Case File/ Individual Files	*As Expected*	*As Expected*
Case File Data Protection: Modify Case Data	*NA*	*NA*
SQLite Data: Report Active Data	*NA*	*NA*
SQLite Data: Run SQLite Commands	*NA*	*NA*

Table 3b: iOS Devices