June 2022

Test Results for Mobile Device Acquisition Tool:
Elcomsoft iOS Forensic Toolkit v7.40 / Phone Viewer v5.33

Contents

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 (NIJ), and the National Institute of Standards and Technology (NIST) Special Programs Office 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 DHS'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 website (https://www.cftt.nist.gov/).

This document reports the results from testing Elcomsoft iOS Forensic Toolkit v7.40 / Phone Viewer v5.33 across supported mobile devices.

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 / Phone Viewer

Software Version: iOS Forensic Toolkit v7.40 / Phone Viewer v5.33

Supplier: Elcomsoft

WWW: elcomsoft.com

1 Results Summary

Elcomsoft iOS Forensic Toolkit v7.40 / Phone Viewer v5.33 was tested for its ability to acquire active data from the internal memory of supported mobile devices.

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. Elcomsoft's Phone Viewer is limited in it's parsing capabilities for full file system data extractions. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

***Personal Information Management (PIM) data*:**

Data (i.e., address, birthdate) associated with Address book entries are not reported. (Devices: *iPhone 7, iPhone 8, iPhone X, iPhone XR, iPhone SE, iPhone 11, iPad Air*)

Stand-alone Files:

Stand-alone files (audio, documents) are not reported. (Devices: *iPhone 7, iPhone 8, iPhone X, iPhone XR, iPhone SE, iPhone 11, iPad Air*)

Social Media Data:

- Social media related data (i.e., Facebook, Twitter, LinkedIn, Instagram) is not reported. (Device: *iPhone 7*)
- Social media related data (i.e., Facebook, LinkedIn, Instagram, Pinterest, Snapchat, Twitter, WhatsApp) is not reported. (Devices: *iPhone 8, iPhone X*)
- Social media related data (i.e., Facebook, Twitter, LinkedIn, Pinterest) is not reported. (Device: *iPad Air*)

Internet Data:

Email data is not reported. (Devices: *iPhone 7, iPhone 8, iPhone X, iPad Air*)

GPS Location Data:

GPS related data (coordinates, locations, geotagged pictures/videos) are not reported. (Devices: *iPhone XR, iPhone SE, iPhone 11, iPad Air*)

For more test result details see section 4.

2 Mobile Devices

The following table lists the mobile devices used for testing Elcomsoft iOS Forensic Toolkit v7.40 / Phone Viewer v5.33.

Make	Model	OS	Extraction Type	Firmware	Network
Apple iPhone	7	iOS 10.2 (14C92)	Full File System/iTunes Backup	1.33.00	CDMA
Apple iPhone	8	iOS 11.3.1 (15E30277)	Full File System/iTunes Backup	1.89.00	CDMA
Apple iPhone	X	iOS 11.3.1 (15E302)	Full File System/iTunes Backup	1.89.00	CDMA
Apple iPhone	XR	iOS 15.1 NQCK2LL/A	iTunes Backup	7.02.00	CDMA
Apple iPhone	SE	iOS 15.1 (MX9N2LL/A)	iTunes Backup	1.06.00	CDMA
Apple iPhone	11	iOS 15.1 (15E302)	iTunes Backup	3.0.00	CDMA
Apple iPad	Air	iOS 11.2.1 (11D167)	Full File System/iTunes Backup	2.18.02	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 iOS Forensic Toolkit v7.40 / Phone Viewer v5.33 was installed on Windows 10 Pro version 10.0.19042.1586.

3.2 Internal Memory Data Objects

Elcomsoft iOS Forensic Toolkit v7.40 / Phone Viewer v5.33 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; 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*

Data Objects	Data Elements
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. Section 4.1 identifies the mobile device operating system type, media, and the make and model of mobile devices used for testing Elcomsoft iOS Forensic Toolkit v7.40 / Phone Viewer v5.33.

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 iOS mobile devices within each test case. Each individual sub-category row shows 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 of 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 either does not provide support for the acquisition for a particular data element or the data extraction performed does not return specific data elements.

4.1 iOS Mobile Devices

The internal memory contents for iOS devices were acquired and analyzed with Elcomsoft iOS Forensic Toolkit v7.40 / Phone Viewer v5.33. The data extraction type selected for all iOS devices is defined above in Table 1.

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

- Data (i.e., address, birthdate) associated with individual contacts were not reported for all iOS devices.
- Stand-alone files (i.e., audio, documents) were not reported for all iOS devices.
- Social media related data (i.e., Facebook, Twitter, LinkedIn, Instagram) is not reported for the iPhone 7.
- Social media related data (i.e., Facebook, LinkedIn, Instagram, Pinterest, Snapchat, Twitter, WhatsApp) is not reported for the iPhone 8 and iPhone X.
- Social media related data (i.e., Facebook, Twitter, LinkedIn, Pinterest) is not reported for the iPad Air.
- Email data is not reported for the iPhone 7, iPhone 8, iPhone X, and iPad Air.
- GPS related data (i.e., longititude, latitude coordinates) are not reported for the iPhone XR, iPhone SE, iPhone 11, and iPad Air.

See Table 3 below for more details. Devices marked with an * indicate both a Full File System data extraction and iTunes Backup data extraction were performed. Devices without an * indicate only an iTunes Backup data extraction was performed.

iOS Forensic Toolkit v7.40 / Phone Viewer v5.33

Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*						
		iPhone 7*	iPhone 8*	iPhone X*	iPhone XR	iPhone SE	iPhone 11	iPad Air v11.2.1*
Acquisition	Acquire All	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Disrupted	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Reporting	Preview-Pane	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	Generated Reports	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Equipment/ User Data	IMEI/MEID/ ESN	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
	MSISDN	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
PIM Data	Contacts	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*	*Partial*
	Calendar	*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*
Call Logs	Incoming	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Outgoing	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
	Missed	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*NA*
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*	*As Expected*	*As Expected*
	Audio	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*
	Video	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*	*As Expected*
Application Data	Documents (txt, pdf files)	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*

iOS Forensic Toolkit v7.40 / Phone Viewer v5.33								
Test Cases – Internal Memory Acquisition		*Mobile Device Platform: iOS*						
		iPhone 7*	iPhone 8*	iPhone X*	iPhone XR	iPhone SE	iPhone 11	iPad Air v11.2.1*
Social Media Data	Facebook	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*NA*	*NA*	*Not As Expected*
	Twitter	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*NA*	*NA*	*Not As Expected*
	LinkedIn	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*NA*	*NA*	*Not As Expected*
	Instagram	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*NA*	*NA*	*NA*
	Pinterest	*NA*	*Not As Expected*	*Not As Expected*	*NA*	*NA*	*NA*	*Not As Expected*
	SnapChat	*NA*	*Not As Expected*	*Not As Expected*	*NA*	*NA*	*NA*	*NA*
	WhatsApp	*NA*	*Not As Expected*	*Not As Expected*	*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	*Not As Expected*	*Not As Expected*	*Not As Expected*	*NA*	*NA*	*NA*	*Not As Expected*
GPS Data	Coordinates/ Geo-tagged	*As Expected*	*As Expected*	*As Expected*	*Not As Expected*	*Not As Expected*	*Not As Expected*	*Not 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	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Case File Data Protection	Modify Case Data	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
SQLite Data	Report Active Data	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
	Run SQLite Commands	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*

Table 3: iOS Devices