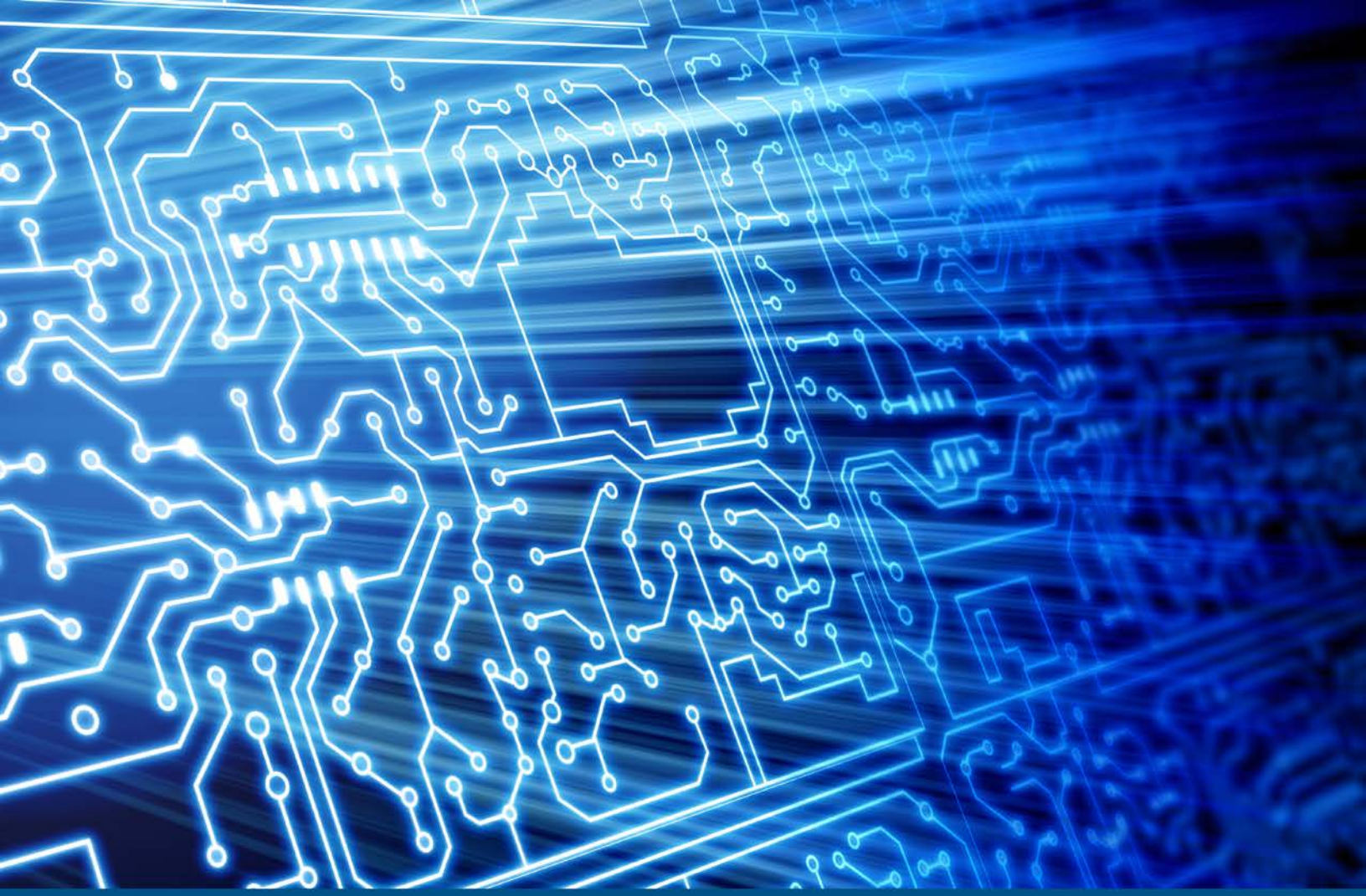

# viaExtract v2.5

Test Results for Mobile Device Acquisition Tool

*December 31, 2014*

Homeland Security

Science and Technology

This report was prepared for the Department of Homeland Security Science and Technology Directorate Cyber Security Division by the Office of Law Enforcement Standards of the National Institute of Standards and Technology.

For additional information about the Cyber Security Division and ongoing projects, please visit www.cyber.st.dhs.gov**.**

**December 2014**

# Test Results for Mobile Device Acquisition Tool:
viaExtract v2.5

## Contents

## 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 Law Enforcement Standards Office (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation (FBI), 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 (ICE), U.S. Customs and Border Protection (CBP) and U.S. Secret Service (USSS). 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 viaExtract v2.5 across Android mobile phones. The images captured from the test runs are available at the CFREDS Web site (http://www.cfreds.nist.gov).

Test results from other tools can be found on the DHS S&T-sponsored digital forensics Web site (http://www.cyberfetch.org/).

## 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. The full test data is available at http://www.cftt.nist.gov/mobile_devices.htm.

# Test Results for Mobile Device Acquisition Tool

| | |
|---|---|
| Tool Tested: | viaExtract |
| Software Version: | v2.5 |
| Supplier: | viaForensics |
| Address: | 1046 Lake Street Oak<br>Park, IL 60301 |
| Tel: | (312) 878-1100 |
| Fax: | (312) 268-7281 |
| WWW: | https://viaforensics.com |

## 1 Results Summary

viaExtract is designed for logical and physical acquisitions (rooted devices), data analysis and report management from Android mobile devices.

The tool was tested for its ability to acquire active and deleted data from the internal memory of supported mobile devices. Except for the following anomalies, the tool acquired all supported data objects completely and accurately for all mobile devices tested.

***Equipment / Subscriber related data*:**

- Equipment and subscriber related data (i.e., MSISDN) were not reported. (Devices: *Android*)
- The ICCID was not reported (Devices: *Galaxy S3, HTC One, Galaxy S4)*

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

- Call log data was not reported. (Devices: *Android*)
- Graphics files associated with address book entries were not reported. (Devices: *Android*)
- Memo entries were not reported. (Devices: *Android*)

***Application / Social Media related data*:**

- Application and Social media related data were not reported. (Devices: *Android*)

For more test result details see section 4.

# 2 Mobile Devices

The following table lists the mobile devices used for testing viaExtract.

| Make | Model | OS | Firmware | Network |
|---|---|---|---|---|
| Samsung Galaxy S3 | SGH-1747 | Android 4.1.2 | 1747UCDMG2 | GSM |
| Samsung Galaxy S4 | SGH-M919 | Android 4.2.2 | M919UVUAMDL | GSM |
| Samsung Galaxy S5 | SM-G900V | Android 4.2.2 | G900V.05 | CDMA |
| HTC One | HTCC6525LVW | Android 4.2.2 | 0.89.20.0222 | GSM |
| HTC One | HTC One | Android 4.1.2 | 4A.17.3250.20_10.40.1150.04L | CDMA |
| Samsung Galaxy Note 3 | SM-N900V | Android 4.3 | N900V.07 | CDMA |
| Nexus 4 | Nexus 4 | Android 4.3 | JWR66Y | GSM |

**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 and UICCs.

## *3.1 Execution Environment*

viaExtract v2.5 was installed by downloading the ISO file from viaforensics.com.

## *3.2 Internal Memory Data Objects*

viaExtract 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* |

| Data Objects | Data Elements |
|---|---|
| | *Deleted Entry* |
| | *Non-ASCII Entry* |
| PIM Data | |
| Datebook/Calendar | *Regular Length* |
| Memos | *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-ASCII 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* |

| Data Objects | Data Elements |
|---|---|
| Internet Data | |
| | *Visited Sites* |
| | *Bookmarks* |
| Location Data | |
| | *GPS Coordinates* |
| Social Media Data | |
| | *Facebook* |
| | *Twitter* |
| | *LinkedIn* |

**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 (i.e., Android) and the make and model of mobile devices used for testing viaExtract v2.5.

The *Test Cases* column (internal memory acquisition) in section 4.1 are 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 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 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 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 Android Mobile Devices

The internal memory contents for Android devices were acquired and analyzed with viaExtract v2.5.

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

- Equipment and subscriber related data (i.e., MSISDN) were not reported. (Devices: *Android*)
- The ICCID was not reported (Devices: *Galaxy S3, HTC One, Galaxy S4)*
- Graphic files associated with *address book entries* were not reported
- *Memos* were not reported
- *Call logs* (i.e., incoming, outgoing, missed) were not reported
- Documents (i.e., text, pdf) and Social Media related data (i.e., facebook, twitter, linkedin) were not reported

See Table 4 below for more details.

| **viaExtract v2.5** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Test Cases – Internal Memory Acquisition** | | *Mobile Device Platform: Android* | | | | | | |
| | | Galaxy S3 *GSM* | Galaxy S4 *GSM* | Galaxy S5 *CDMA* | Galaxy Note 3 CDMA | HTC One *GSM* | HTC One *CDMA* | Nexus 4 *GSM* |
| **Connectivity** | Non Disrupted | *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 | *As Expected* | *As Expected* | *NA* | *NA* | *As Expected* | *NA* | *As Expected* |
| | MEID/ESN | *NA* | *NA* | *As Expected* | *As Expected* | *NA* | *As Expected* | *NA* |
| | MSISDN | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not 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* |
| | To-Do List/ Tasks | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* |

| viaExtract v2.5 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Test Cases – Internal Memory Acquisition** | | *Mobile Device Platform: Android* | | | | | | |
| | | Galaxy S3 *GSM* | Galaxy S4 *GSM* | Galaxy S5 *CDMA* | Galaxy Note 3 CDMA | HTC One *GSM* | HTC One *CDMA* | Nexus 4 *GSM* |
| | Memos | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* |
| **Call Logs** | Incoming | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* |
| | Outgoing | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* |
| | Missed | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not 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* | *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* |
| **Application Data** | Documents | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* |
| | Spreadsheets | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* |
| | Presentations | *NA* | *NA* | *NA* | *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* |
| **Social Media Data** | Facebook | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* |
| | Twitter | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *As Expected* | *Not As Expected* | *Not As Expected* |
| | LinkedIn | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* | *Not As Expected* |
| **Acquisition** | Acquire All | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* |
| | Selected All | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* |
| | Select Individual | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* |
| **Case File** | Modify Case | *As* | *As* | *As* | *As* | *As* | *As* | *As* |

| viaExtract v2.5 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Test Cases – Internal Memory Acquisition** | | *Mobile Device Platform: Android* | | | | | | |
| | | Galaxy S3 *GSM* | Galaxy S4 *GSM* | Galaxy S5 *CDMA* | Galaxy Note 3 CDMA | HTC One *GSM* | HTC One *CDMA* | Nexus 4 *GSM* |
| **Data Protection** | Data | *Expected* | *Expected* | *Expected* | *Expected* | *Expected* | *Expected* | *Expected* |
| **Physical Acquisition** | Readability | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* |
| | Deleted File Recovery | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* |
| **Non-ASCII Character** | Reported in native format | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* |
| **Hashing** | Hashes reported for acquired data objects | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* | *As Expected* |
| **GPS Data** | Coordinates (Long/Lat) | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* | *NA* |

**Table 3: Android Mobile Devices**