The attached DRAFT document (provided here for historical purposes), released on March 26, 2018, has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-202**

Title: ***Quick Start Guide for Populating Mobile Test Devices***

Publication Date: **May 2018**

- Final Publication: https://doi.org/10.6028/NIST.SP.800-202 (which links to https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-202.pdf).
- Related Information on CSRC:
  Final: https://csrc.nist.gov/publications/detail/sp/800-202/final

NIST Special Publication 800-202

Quick Start Guide for Populating Mobile Test Devices

Rick Ayers
Benjamin Livelsberger
Barbara Guttman

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-202

Quick Start Guide for Populating Mobile Test Devices

Rick Ayers
Benjamin Livelsberger
Barbara Guttman
Software and Systems Division
Information Technology Laboratory

March 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-202
Natl. Inst. Stand. Technol. Spec. Publ. 800-202, 29 pages (March 2018)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *March 26, 2018* through *April 25, 2018*

National Institute of Standards and Technology
Attn: Software and Systems Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8970) Gaithersburg, MD 20899-8970
Email: sp800-202-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This guide provides procedures for documenting and populating various data elements typically found within the contents of a mobile device, e.g., mobile phone, tablet, etc. The guide discusses techniques and considerations for preparing the internal memory of a mobile device for use in testing a mobile forensic tool.

Keywords

Computer Forensic Tool Testing; Digital Forensics; Federated Testing; Mobile Forensics

Acknowledgments

The authors, Rick Ayers, Benjamin Livelsberger and Barbara Guttman from NIST wish to thank colleagues who reviewed drafts of this document. In particular, our appreciation goes to Craig Russell and Jenise Reyes from NIST for their technical support and written contributions to this document. Our appreciation also goes out to Sam Brothers from The MITRE Corporation and Daren Melson for their assistance on technical issues that arose in our work. The authors would also like to thank all others who assisted with our review process.

Audience

The intended audience ranges from law enforcement to forensic practitioners and examiners testing and utilizing digital forensic tools often used in incident response and criminal investigations.

Table of Contents

List of Appendices

List of Tables

1 Introduction

1.1 Document Scope and Purpose

This guide describes how to populate a mobile device as part of testing a mobile forensic tool. It was built to be used with Federated Testing, but can also be used to populate a device for use with other test approaches. The Federated Testing project (https://www.cftt.nist.gov/federated-testing.html) is an expansion of the Computer Forensics Tool Testing (CFTT) Program at NIST which provides digital forensics investigators and labs with test materials for forensic tool testing. The goal of Federated Testing is to help digital forensics investigators to test the tools that they use in their labs and to enable sharing of tool test results within the digital forensics community. The goals of this guide are twofold: 1) provide guidance for how to populate (place test data on) a moble device for use in forensic tool testing and 2) provide guidance to select data elements for inclusion that ensure effective testing.

There are two strategies for populating mobile test devices, e.g., mobile phones, tablets, etc.: 1) populate a new or previously sanitized device or 2) start with a used device and add content as needed. This guide first describes the major data types and how to populate them onto the test device. Appendix B is both a template that should be filled out for each device to document the device's content prior to testing and a specification of properties that each data element should meet. This "ground truth" provides the "expected results" for checking the ability of the tool being tested to obtain all of the device's contents. Appendix C is a sample of a template filled out with appropriate data elements.

This guide will step you through populating and documenting your test devices. This needs to be done for each mobile device. You should select data types that are relevant to the cases seen in your lab. You do not need to include all of the data types. You can include other relevant data types by adding a section to Appendix B.

Used devices may include numerous data elements (e.g., contact entries, call logs, text messages, pictures, etc.). While a device may contain hundreds of a specific data type (e.g., contact entries), users should concentrate on documenting a representative portion of data elements with the required data properties relevant to testing within Appendix B. You only need to populate data where the data element does not already exist.

1.2 Document Organization

The guide is divided into the following sections and appendices describing how to document/populate data for a mobile device and a SIM/UICC:

- Section 2: Document Device Data
- Section 3: Personal Information Management (PIM) Data: Contacts, Calendar & Memos
- Section 4: Stand-alone Data Files
- Section 5: Call Logs
- Section 6: Text Messages
- Section 7: MMS Messages
- Section 8: Location Data

- Section 9: Browser/Email Data
- Section 10: Social Media Data
- Section 11: Other Applications of Interest
- Section 12: SIM/UICC Card
- Appendix A: Acronyms
- Appendix B: Mobile Device Data Documentation - provides users with guidance on specific data properties for each data element type and a blank template to be used to document target mobile devices and/or SIM/UICC data.
- Appendix C: Mobile Device Data Example - offers example data values that may be used to populate a target mobile device and/or SIM/UICC.

NOTE: The status of data populated onto a mobile device and/or a SIM/UICC may either be classified as Active or Deleted. Deleted data objects may be recovered by a mobile forensic tool if they are not overwritten. To prevent overwriting of data objects that are intended to be recovered, do NOT delete data objects populated onto a mobile device and/or SIM/UICC until data population has been completed.

For a more in-depth view on data population refer to CFTT's Mobile Device Data Population Setup Guide https://www.cftt.nist.gov/documents/Mobile Device Data Population Setup Guide.pdf.

2 Document Device Data

Document the equipment (i.e., IMEI) and subscriber (i.e., MSISDN/phone number) data by navigating to the mobile device *Settings* menu. The *Settings* menu is often identified by a gear shaped icon. Equipment and subscriber data may be in a subfolder such as *General* or *About Phone*.

Note: For mobile devices that allow for easy battery removal - the IMEI is also commonly located on a sticker within the battery cavity beneath the battery. For some makes/models of mobile devices the IMEI can be retrieved by entering: *#06# on the keypad.

Document Device Data in Appendix B.

3 Personal Information Management (PIM) Data: Contacts, Calendar & Memos

Populating PIM data onto a mobile device does not require an active cellular subscription. Although, if network connectivity can be established, synchronization of supported data elements with an email account speeds up this process.

Different methods exist for data population, such as manual input or synchronization with an email account.

Synchronizing data from an existing email account to a mobile device requires network connectivity. Support for this method will vary based on make/model of the device.

Note: Synchronization of Contacts, Calendar and Memos with an existing email account may be accomplished by enabling specific data types within the mobile devices email client settings. Once this data is enabled, and the email account is accessed from the mobile device, the sync process should occur. It is recommended to set up a unique email account designed specifically for data synchronization.

Note: Non-Latin text (Non-English, e.g., Chinese, Arabic, Russian, etc.) can be readily created with language translation tools from a web-browser and then copied and pasted.

Document the PIM data in Appendix B.

4 Stand-alone Data Files

Stand-alone data files (e.g., audio, graphic, video) can be populated onto a mobile device using its native applications (i.e., camera, microphone).

Note: If the mobile device has network connectivity, stand-alone files (audio, graphic, video, documents, etc.) may be populated onto the target mobile device by downloading them from an email account.

Document Stand-alone Data Files in Appendix B.

5 Call Logs

When populating mobile devices with call log data, it is useful to obtain two devices. A sending device, and a target device. Missed calls are populated onto the target device by placing a call from a sending device and not answering from the target device. Incoming calls are populated by answering the call from the target device and documenting the date/time and the duration of the call. Outgoing calls are placed from the target device to secondary lines.

Document Call Logs in Appendix B.

6 Text Messages

Populating mobile devices with text messages requires two mobile devices. A sending device, and a target device. Text messages may be categorized as either Short Messages Service (SMS) or Enhanced Message Service (EMS) messages.

SMS messages are solely textual based messages containing less than 160 characters. EMS messages are an extension of SMS and support text messages of 160 or more characters.

Incoming messages are populated onto the target device by sending the message from a sending device. Outgoing messages are populated by sending a message from the target device to a secondary device.

In addition to the text message, document phone numbers, date/time, and the status (i.e., read, unread, deleted).

Note: Text messages are categorized with a status of either: Read, Unread, or Deleted. To establish messages with a status of read, open and observe the message on the screen. Messages with a status of Unread are accomplished by not reading/opening the message. Messages with a status of Deleted are accomplished by deleting a specific message after the phone has been entirely populated.

Document Text Messages in Appendix B.

7 MMS Messages

MMS messages are populated onto the target device similar to text messages as described above in Section 6. MMS messages contain either an audio, graphic or a video attachment - with or without a text message.

Incoming MMS messages are populated onto the target device by sending MMS (audio, graphic, video) messages from a sending device. Outgoing MMS messages can be created using native applications (i.e., camera, microphone) and populated by sending a message from the target device to a secondary device. In addition to the text message, document phone numbers, date/time, and the status (i.e., read, unread, deleted).

Note: MMS messages are categorized with a status of either: Read or Unread. To establish messages with a status of read, open and observe the message on the screen. Messages with a status of Unread are accomplished by not reading/opening the message. Messages with a status of Deleted are accomplished by deleting a specific message after the phone has been entirely populated.

Document MMS Messages in Appendix B.

8 Location Data

Location related data is populated onto a mobile device by enabling location services. Initiate a GPS related application from the target device, enter a destination and begin the route.

Pictures and videos may also contain location related data. The mobile device's camera security settings will determine if this feature is supported. For devices supporting "geotagged" pictures and video, populate the target device by taking photographs and video while documenting the location.

Document Location Data in Appendix B.

9 Browser/Email Data

Internet related data may be populated onto mobile devices by opening a browser on the device (e.g., Chrome, Safari). The following data elements: Internet history, bookmarks are populated onto the target device by visiting and bookmarking selected URLs.

Email related data may be populated onto supported devices by opening an email client and sending/receiving emails to/from the device.

Document Browser/Email Data in Appendix B.

10 Social Media Data

Mobile devices support a variety of social media applications such as: Facebook, LinkedIn, Twitter, and Instagram.

Individual social media accounts can be created from either a personal computer or mobile device with network connectivity. It is recommended to create two social media accounts (e.g., mobile_1, mobile_2). Creating two accounts provides the user with the ability to populate the target device with dialogue such as personal messages (PMs) between the two accounts. In addition to PMs; faux profile information (e.g., high school, college, employer, current city, hometown), picture albums, status updates, profile pictures, video, etc. should be created by accessing both accounts (for each social media app) on the target device.

Available features of each social media application will vary. Typically, applications provide users with the ability to create a profile (picture, background information, etc.) of the account and to share status information that may or may not include: pictures, video or audio files.

Document Social Media Data in Appendix B.

11 Other Applications of Interest

Other types of application related data (not covered in sections 2 - 10) may be populated to a mobile device (e.g., reminders, wallet, cloud storage, productivity, organization, etc.). Consider populating a mobile device with application data critical to your casework. Selection of apps should focus on ones that are not covered in previous sections.

Document Other Applications of Interest in Appendix B.

12 SIM/UICC Card

The make and model a mobile device determines if data i.e., Contacts/Abbreviated Dialing Numbers (ADN), Last Numbers Dialed (LND) and text (SMS, EMS) messages may be stored on a SIM/UICC. Newer devices typically store this information within the mobile device internal memory.

If the target device has a SIM/UICC card capable of storing ADNs, LNDs, SMS, EMS data; manually populate the SIM/UICC by performing the following:

1) Export Contact information from the internal memory of the device to the SIM/UICC. This typically is done by clicking on a Contact/Address book entry and selecting copy/export and selecting the SIM as the location.
2) LNDs – place outgoing calls from the target device.
3) Incoming text messages (SMS, EMS) – send messages from a secondary device to the target device.

Note: Document subscriber and equipment related data (e.g., ICCID, IMSI) after successfully acquiring the contents of the target SIM/UICC.

Document SIM/UICC Card in Appendix B.

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

ADN	Abbreviated Dialing Numbers
AVI	Audio Video Interleave
BMP	Bitmap Image File
DOC	Document
EMS	Enhanced Message Service
ESN	Electronic Serial Number
FLV	Flash Video
GIF	Graphics Interchange Format
GPRSLOCI	General Packet Radio Service Location
GPS	Global Positioning System
ICCID	Integrated Circuit Card Identification
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
JPG	Joint Photographic Experts Group
LND	Last Numbers Dialed
LOCI	Location Information
MEID	Mobile Equipment Identifier
MIN	Mobile Identification Number
MMS	Multi-media Service
MOV	QuickTime Movie
MP3	MPEG (Motion Picture Experts Group) Layer 3
MP4	MPEG Layer-4 Audio

MSISDN	Mobile Station Integrated Services Digital Network
OGG	Ogg Vorbis Audio File
PDF	Portable Document Format
PIM	Personal Information Management
PM	Personal Message
PNG	Portable Network Graphics
PPT	Power Point File
SIM	Subscriber Identity Module
SMS	Short Message Service
SPN	Service Provider Name
TXT	Text File
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
WAV	WaveForm Audio File
WMA	Windows Media Audio

365

Appendix B—Mobile Device Data Documentaion

Appendix B provides the user with the ability to document data contained on a mobile device and/or SIM/UICC. To record each mobile device a separate appendix B should be used each time.

Table 1: Equipment and Subscriber-related data

Data Element	Data Value
Device Make/Model	
IMEI/MEID/ESN	
MSISDN / MIN	

Table 2: PIM data

Data Objects	Data Properties	Data Value
Contacts/Address Book Entries	Regular length (up to 50 chars)	
	Maximum length (over 50 chars)	
	Special character (!, @, #, $, %, ^, &, *)	
	Blank name	
	Regular length with multiple metadata objects (e.g., graphic, email, URL, Address, Birthday) supported by the device	
	Non-Latin entry	
	Contact groups	
	Deleted entry	
Calendar data	Regular length (up to 50 chars)	
	Maximum length entry (100+ characters)	
	Special character entry	

Data Objects	Data Properties	Data Value
	Blank title entry	
	Deleted entry	
Memo data	Regular length entry (100 characters or less)	
	Maximum length entry (1000 characters+)	
	Deleted entry (100-1000 characters)	

375
376
377

Table 3: Stand-alone data files

Data Objects	Data Properties	Data description/contents
Stand-alone files	Audio	mp3
		wav
		ogg
		wma
	Graphic	bmp
		gif
		jpg
		png
	Video	avi
		flv
		mov
		mp4
	Documents	txt
		doc
		pdf
		ppt
	Audio – Deleted	
	Graphic – Deleted	
	Video – Deleted	
	Documents – Deleted	

378
379

380 **Table 4: Call Log data**

Data Objects	Data Properties	Data Value/Date/Time/Duration
Call Logs	Incoming Calls	
	Outgoing Calls	
	Missed Calls	
	Incoming – Deleted	
	Outgoing – Deleted	
	Missed – Deleted	

381
382
383 **Table 5: Text Messages**

Data Objects	Data Properties	Data Value/Sender/Receiver phone number/Date/Time
SMS/EMS Messages	Incoming SMS/Read	
	Incoming SMS/Unread	
	Incoming SMS/Deleted	
	Incoming EMS/Read (160 characters +)	
	Incoming EMS/Unread (160 characters +)	
	Incoming EMS/Deleted (160 characters +)	
	Outgoing SMS	
	Outgoing group SMS	
	Outgoing SMS/Deleted	

Data Objects	Data Properties	Data Value/Sender/Receiver phone number/Date/Time
	Outgoing EMS (160 characters +)	
	Outgoing group EMS (160 characters +)	
	Outgoing EMS/Deleted (160 characters +)	

384
385
386

Table 6: Multi-media Messages

Data Objects	Data Properties	Data Value/Sender/Receiver phone number/Date/Time
MMS Messages	Incoming audio MMS	
	Incoming graphic MMS	
	Incoming video MMS	
	Outgoing audio MMS	
	Outgoing graphic MMS	
	Outgoing video MMS	

387
388
389

Table 7: Location data

Data Objects	Data Properties	Data Value
Navigation (Device Specific)	Waypoints (longitude/latitude)	
	Checking In (places of interest)	
	Pictures/Video (geotagged)	
	Trip (destination)	

Data Objects	Data Properties	Data Value

Table 8: Browser/email data

Data Objects	Data Properties	Data Value
Bookmarks/History/Email	Visited Sites:	
	Bookmarked Sites:	
	Email data:	

Table 9: Social Media related data

Data Objects	Data Properties	Data Value
Profile information, Status updates, personal messages, etc.	Application 1, e.g., Facebook/Facebook messenger	
	Application 2, e.g., Twitter	
	Application 3, e.g., LinkedIn	
	Application 4, e.g., Instagram	

397 **Table 10: Other applications of interest**

Data Objects	Data Properties	Data Value
Application related data	Application 1 (e.g., reminders)	
	Application 2 (e.g., Productivity)	
	Application 3 (e.g., Organization)	

398
399
400 ***Note: Populating data onto SIM/UICCs is dependent upon the make and model of mobile***
401 ***device.***
402 **Table 11: SIM/UICC data**

Data Element		Data Value
ICCID		
Service Provider Name (SPN)		
IMSI		
Abbreviated Dialing Numbers (ADNs)	Maximum Length	
	Special Character	
	Blank Name	
	Non-ASCII Entry	
	Regular Length	
Last Numbers Dialed (LNDs)		
Incoming SMS Messages	Read	
	Unread	
	Non-ASCII	
	Deleted	
Incoming EMS Messages (over 160 chars)	Read	
	Unread	
	Non-ASCII	
	Deleted	
LOCI		
GPRSLOCI		

403

Appendix C—Mobile Device Data Example

Appendix C – contains an example/template of a dataset used for populating the internal memory and associated media i.e., SIM/UICC of a test device.

Table 12: PIM data example

Data Objects	Data Properties	Data Value
Contacts/Address Book Entries	Regular length (up to 50 chars)	Eddie Van Halen, 5150515051
	Maximum length (over 50 chars)	John Jacob Jingle Heimer Schmidt That's My Name Too Whenever I Go Out The People Always Shout John Jacob Jingle Heimer Schmidt, 8988675309
	Special character (!, @, #, $, %, ^, &, *)	*, 8887771212
	Blank name	8785551111
	Regular length with multiple metadata objects (e.g., graphic, email, URL, Address, Birthdate) supported by the device.	Stevie Ray Vaughn, 1234567890, work: stevie@srv.com, address: 1234 Main Street, Dallas, TX, SRV Birthday: October 3, 1954 
	Non-Latin entry	阿恶哈拉, +86 35 8 763 30 07 Aurélien, +33 22 6 555 20 20
	Contact groups	27 Club: Jimi Hendrix*, Stevie Ray Vaughn*, John Bonham
	Deleted entry	John Bonham, 9878767654
Calendar data	Regular length (up to 50 characters)	Date/Time: Location: Los Angeles Type: Meeting Title: Rush Concert
	Maximum length entry (100+ characters)	Date/Time: Type: Reminder Title: Van Halen were scheduled to perform forty shows on their 2007 tour with David Lee Roth after much success in the early 80s with David Lee Roth as their front man for Van Halen!!
	Special character entry	Date/Time: e.g.,!, @, #, $, %, ^, &, *
	Blank title entry	Date/Time:

Data Objects	Data Properties	Data Value
		Type: Reminder
	Deleted entry	Date/Time: Hendrix Summer of Love Documentary
Memo data	Regular length entry	(100 characters or less)
	Long entry	(1000 characters +)
	Deleted entry	(100 – 1000 characters)

409
410
411

Table 13: Stand-alone data files example

Data Objects	Data Properties	Data Value
Stand-alone files	Audio	*Supported audio files (e.g., mp3, wav, ogg, wma)*
	Graphic	*Supported graphic files (e.g., bmp, gif, jpg, png)*
	Video	*Supported video files (e.g., avi, flv, mov, mp4)*
	Documents	*Supported document files (e.g., txt, doc, pdf, ppt)*
	Audio – Deleted	*Deleted audio file*
	Graphic – Deleted	*Deleted graphic file*
	Video – Deleted	*Deleted video file*
	Documents – Deleted	*Deleted document file*

412
413
414

Table 14: Call Log data example

Data Objects	Data Properties	Data Value/Date/Time/Duration
Call Logs	Incoming Calls	(301) 555-0101 / April 12, 2017 2:07pm / 10 minutes
		(703) 555-0102 / April 12, 2017 2:20pm / Canceled call
		(103) 555-0103 / April 12, 2017 2:21pm / 2 seconds
	Outgoing Calls	(xxx) xxx-xxxx / April 12, 2017 2:25pm / 3 seconds
		(xxx) xxx-xxxx / April 12, 2017 2:26pm / 2 minutes, 3 seconds
		(xxx) xxx-xxxx / April 12, 2017 2:30pm / 10 seconds
	Missed Calls	(xxx) xxx-xxxx / April 12, 2017 3:01pm
		(xxx) xxx-xxxx / April 12, 2017 3:03pm
		(xxx) xxx-xxxx / April 12, 2017 3:07pm
	Incoming – Deleted	(103) 555-0103 / April 12, 2017 3:09pm / 2 seconds

Data Objects	Data Properties	Data Value/Date/Time/Duration
	Outgoing – Deleted	(xxx) xxx-xxxx / April 12, 2017 3:10pm / 3 seconds
	Missed - Deleted	(xxx) xxx-xxxx / April 12, 2017 3:15pm

415
416
417

Table 15: Text Messages example

Data Objects	Data Properties	Data Value/Sender/Receiver phone number/Date/Time
SMS/EMS Messages	Incoming SMS/Read	The following SMS message is a read incoming message sent from another device / (301) 555-0102 / April 12, 2017 3:15pm
	Incoming SMS/Unread	The following SMS message is an unread message sent from another device / (301) 555-0102 / April 12, 2017 3:16pm
	Incoming SMS/Deleted	This is a deleted incoming message sent from another device / (301) 555-0102 / April 12, 2017 3:17pm
	Incoming EMS/Read	Incoming read active extended SMS message. This is an incoming SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message. / (301) 555-0102 / April 12, 2017 3:17pm
	Incoming EMS/Unread	Incoming unread active extended SMS message. This is an incoming SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message. (301) 555-0102 / April 12, 2017 3:18pm
	Incoming EMS/Deleted	Incoming deleted extended SMS message. This is a deleted incoming SMS message sent from another device to determine if the forensic application has the ability to acquire and report deleted incoming SMS messages. / (301) 555-0102 / April 12, 2017 3:20pm
	Outgoing SMS	The following SMS message is an active outgoing message sent to another device / (301) 555-0101 / April 12, 2017 3:20pm
	Outgoing group SMS	The following SMS message is an active outgoing group message sent to multiple

Data Objects	Data Properties	Data Value/Sender/Receiver phone number/Date/Time
		recipients / (301) 555-0101 and (301) 555-0102 / April 12, 2017 3:21pm
	Outgoing SMS/Deleted	This is a deleted outgoing message sent to another device / (301) 555-0101 / April 12, 2017 3:21pm
	Outgoing EMS	Outgoing active extended SMS message. This is an outgoing SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message. / (301) 555-0101 / April 12, 2017 3:22pm
	Outgoing group EMS	Outgoing active extended SMS message. This is an outgoing SMS message sent to multiple recipients that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message. / (301) 555-0101 and (301) 555-0102 / April 12, 2017 3:23pm
	Outgoing EMS/ Deleted	Outgoing deleted extended SMS message. This is a deleted outgoing SMS message sent to another device to determine if the forensic application has the ability to acquire and report deleted outgoing SMS messages. / (301) 555-0101 / April 12, 2017 3:25pm

418
419
420

Table 16: Multi-media Messages example

Data Objects	Data Properties	Data Value/Sender/Receiver phone number/Date/Time
MMS Messages	Incoming audio MMS	Incoming sound byte message *attachment: audio file* / (301) 555-0101 / April 12, 2017 4:00pm
	Incoming graphic MMS	Incoming graphic message *attachment: graphic file* / (301) 555-0101 / April 12, 2017 4:01pm
	Incoming video MMS	Incoming video message *attachment: video file* / (301) 555-0101 / April 12, 2017 4:03pm

Data Objects	Data Properties	Data Value/Sender/Receiver phone number/Date/Time
	Outgoing audio MMS	Outgoing sound byte message *attachment: audio file* / (301) 555-0101 / April 12, 2017 4:07pm
	Outgoing graphic MMS	Outgoing graphic message *attachment: graphic file* / (301) 555-0101 / April 12, 2017 4:09pm
	Outgoing video MMS	Outgoing video message *attachment: video file* / (301) 555-0101 / April 12, 2017 4:12pm

Table 17: Location Data example

Data Objects	Data Properties	Data Value
Navigation (Device Specific)	Waypoints	*Longitude/Latitude coordinates*
	Checking In	*Social media*
	Pictures/Video	*Geotagged*
	Trip	*Trip Advisor*

Table 18: Browser/email data example

Data Objects	Data Properties	Data Value
Bookmarks/History/Email	Visited Sites:	*History of various sites navigated to*
	Bookmarked Sites:	*Active and deleted entries*
	Email data:	*Cached data to the phone*

Table 19: Social Media related data example

Data Objects	Data Properties	Data Value
Profile information, Status updates, personal messages, etc.	Facebook/Facebook messenger	Profile related data (picture, bio), Status updates, personal messages, etc.
	Twitter	Profile related data (picture, bio), Tweets, personal messages, etc.
	LinkedIn	Profile related data (picture, bio), personal messages, etc.
	Instagram	Profile related data (picture, bio), Posted pictures, videos, etc.

431
432

Table 20: Other applications of interest example

Data Objects	Data Properties	Data Value
Application related data	Application 1 (e.g., reminders)	
	Application 2 (e.g., Productivity)	
	Application 3 (e.g., Organization)	

433
434
435 ***Note: Populating data onto SIM/UICCs is dependent upon the make and model of mobile***
436 ***device.***
437

Table 21: SIM/UICC data example

Data Element	Data Value
ICCID	*Documented from the SIM/UICC casing*
Sevice Provider Name (SPN)	*Documented from the phone provider*
IMSI	*Documented from the phone settings*
Abbreviated Dialing Numbers (ADNs)	*If supported by mobile device – export internal memory contacts to the SIM/UICC*
Last Numbers Dialed (LNDs)	(301) 555-0101 (703) 555-0102 (103) 555-0103 (401) 555-0104 (205) 555-0105 (207) 555-0106 (280) 555-0107 (109) 555-0108 (404) 555-0109 (616) 555 -0110
SMS Messages (active)	The following SMS message is an active SMS message.
SMS Message (deleted)	The following SMS message is a deleted SMS message.
EMS Messages (over 160 chars)	This is an extended SMS message. Extended SMS messages referred to as EMS messages are messages that dexceeds 160 characters. This message will determine if the forensic

Data Element	Data Value
	application properly reports all characters contained in the message.
Non-ASCII EMS Messages	икра 古老肉شیشلیک Döner kebab sauté
LOCI	*Values are determined by location*
GPRSLOCI	*Values are determined by location*

438
439