March 2016

Mobile Device Data Population Setup Guide

Version 2.0

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 Special Program Office (SPO) 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 the U.S. Department of Homeland Security'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 Web site (http://www.cftt.nist.gov/).

Purpose

This document provides techniques for preparing a mobile device for use in testing mobile forensic data extraction tools. Techniques are described for documenting device intrinsic data (e.g., mobile equipment identifiers), existing user data and how to add user data that has potential to reveal problems during tool testing. There are several factors to consider in preparing a mobile device for testing mobile device forensic data extraction tools:

- Fresh, unused device with no user data
- Phone network connectivity
- PII on device with existing user data

If you know the memory contents of a digital device, then the completeness and accuracy of data returned by a forensic extraction tool can be evaluated. Fresh mobile devices with network connectivity containing no user data are preferred since the tester can populate the device with data as needed. If fresh devices are not available this document provides guidance for documenting existing data on a used device and adding additional known data to support tool testing.

Often times, mobile devices available for testing a mobile forensic tool contain data from a previous account. When using acquired mobile devices with preexisting data, examiners must completely and meticulously document the contents of the mobile device. In addition, if a device has preexisting data that includes *personally identifiable information* (PII), then the PII must be treated in an appropriate manner, e.g., redacted before any public release of a test report. Where possible, PII should be overwritten or replaced with benign test data. While pre-populated devices eliminate the task of populating the internal memory, recoverable data that was previously deleted goes undocumented. Therefore, connectivity (i.e., cellular, WiFi) and the status of the memory (i.e., pre-populated, non-populated) plays a large role in the documentation and data population techniques used. While there are various data population techniques for mobile devices, lack of network connectivity makes data population challenging e.g., the inability to receive incoming calls, text messages, etc. Devices lacking network connectivity must be populated manually or by Bluetooth pairing with another device, if supported.

Two primary techniques that aid in populating a mobile device with network connectivity include: email client pairing and personal computer synchronization software. Pairing a mobile device with an email account allows Contacts, Calendar entries and email attachments (e.g., pictures, audio, video, documents) to be automatically synched and saved to a supported mobile device. Email clients and the variety of synched data elements may vary based upon make and model of mobile device. An email account should be created and populated from a personal computer to be used specifically for data synchronization to the mobile device. The disadvantages for email client synchronization typically are based upon limitations (e.g., email client setup, data elements) of the make and model of mobile device.

Personal computer synchronization software is another technique for populating data onto supported devices. PC sync software provides the user with the ability to transfer data

elements from a personal computer to the mobile device, but is typically limited to supported types of data elements (e.g., pictures, audio, video, documents).

The document is organized by listing the various data types that either may be populated onto a mobile device or already exist within the internal memory of a device. Each section briefly describes data elements and approaches for populating or documenting the internal memory of a mobile device used when testing a mobile forensic data extraction tool. A set of suggested data that can be used to populate a device is included in Appendix A and can be downloaded from the CFReDS web site: http://www.cfreds.nist.gov/.

1 Subscriber / Equipment Data

Subscriber and equipment related data are identifiers useful for uniquely identifying a cellular subscription and physical identification of a mobile device. The International Mobile Station Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), Electronic Serial Number (ESN) are all device identifiers that provide wireless carriers and cell phone manufacturers with the ability to identify specific devices. IMEIs are specific to devices that operate over the GSM network in comparison to MEID/ESN identifiers that require a CDMA network. Sections 1.1 – 1.4 provide additional information on subscriber and equipment related data and where the information can be found for documentation purposes before testing a mobile forensic tool.

1.1 International Mobile Station Equipment Identify (IMEI)

The International Mobile Station Equipment Identity (IMEI) is used for identifying 3GPP (i.e., GSM, UMTS and LTE) and iDEN mobile phones. The IMEI is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the keypad, or by navigating to the devices system information in the settings menu. The IMEI is a device identifier used to help wireless carriers and manufacturers identify specific devices.

1.2 Electronic Serial Numbers / Mobile Equipment Identifiers (ESN/MEID)

Electronic Serial Numbers (ESN) identifies mobile devices operating over a Code Division Multiple Access (CDMA) network for wireless service. ESNs have been phased out in favor of Mobile Equipment Identifiers (MEID). MEIDs are a longer number (i.e., 14 digits) and more similar to the IMEI used in mobile devices operating over the GSM network. Like an IMEI, ESNs/MEIDs are generally printed beneath the battery in the battery cavity or can be found within the settings menu of the mobile device.

1.3 Integrated Circuit ID (ICCID)

The Integrated Circuit Card Identifier (ICCID) is a unique serial number assigned to and stored within the memory of a (U)SIM or Universal Integrated Circuit Card (UICC). Additionally, the ICCID is usually printed on the exterior of (U)SIM or UICC cards.

1.4 Mobile Station International Subscriber Directory Number (MSISDN)

The Mobile Station International Subscriber Directory Number (MSISDN) is an international telephone number assigned to a cellular subscriber. The MSISDN is generally found within the settings menu of the mobile device. The subscriber number can also be documented using caller-id of a known device by placing an outgoing call.

2 Address Book / Contacts

Address book/Contact entries typically contain a contact name and associated mobile number. Additional data for contact entries may include home/work phone numbers, street address, notes, ringtones, picture, etc.

Contact data can be populated onto the internal memory of mobile devices with or without a service contract using one of two techniques: manual or by syncing the contact list with an existing email account (e.g., Gmail, Yahoo, etc.).

Manually populating a mobile device with contact data requires navigating to the mobile device contact menu and adding new contact information using either the keypad on on-screen keyboard. Sections 2.1 – 2.3 provide examples of data types that may be included when creating contact data.

The second technique for populating Address Book / Contacts onto the internal memory of a mobile device involves syncing data with a pre-existing email client (e.g., Gmail, Yahoo, iCloud, etc.). Smart phones often provide users with an option to configure a mobile device email application. Mobile email applications offered vary based on the mobile device, make and model. Mobile email client settings are often located beneath Settings/Mail, Contacts. The Mail, Contacts tab allows users to specify data elements to sync from an existing email client to the mobile device. It is strategic to set up a unique online email account and populate it with the Address Book / Contact information specific for syncing to mobile devices used for explicitly testing.

Syncing the Address Book / Contact information to a pre-existing email account requires mobile device cellular or Wi-Fi connectivity. Once the settings on the mobile device email application are set appropriately, the mobile device needs to establish Internet connectivity via cellular connectivity or by connecting to a router that provides wireless connectivity. The mobile device memory contents will begin to populate upon successfully login via the mobile email client. Verification that the data has been populated onto the mobile device can be performed by opening the Address book / Contacts.

2.1 Contact Name

Various types of contact names should be populated onto the internal memory of the mobile device.

- Long name – over 50 characters or the maximum amount of characters for the first, middle, last names that the mobile device supports
- Regular name – regular length name with the first, middle, and last contact fields populated
- Special character – contact name containing only a special character e.g., *, !, &, %, $, @
- Blank name – contact name is left empty, only a mobile number is provided
- Non-ASCII character contacts – contact entries containing various non-Latin characters
- Deleted contacts – entries that have been deleted from the internal memory of the mobile device

2.2 Contact Phone Number

Contacts should contain various lengths of phone numbers.

- Blank contact number – the contact entry does not contain a phone number
- Regular length contact number – the contact contains an area code, prefix, and subscriber number
- Full contact number – country code, area code, prefix, and subscriber number

2.3 Contact Metadata

Contact entries can contain various types of metadata e.g., email address, street address, URLs, birthdates, pictures, ring-tones, etc. Contacts populated onto the mobile device should contain the following (if supported by the mobile device).

- Email address – various lengths
- Street address – street number, street name, city, state, zip
- URLs – for web pages
- Birthdates – various formats 21 Dec 2012, 12/21/2012
- Pictures – a picture associated with the contact
- Ring-tone – special sound byte associated with the contact
- Additional notes – information specific with the contact
- Deleted data – metadata that has been deleted from the internal memory of the mobile device

3 Personal Information Management Data

Personal Information Management (PIM) data such as datebook/calendar entries, tasks, notes, and memo entries should be populated onto the mobile devices internal memory based upon what application support the mobile device provides. Mobile devices based on operating system, make, manufacturer will vary within the facilities provided to the user. Datebook/calendar entries can either be entered manually or synced with a tethered email client that syncs information between the email client and mobile device. Memo entries can either be manually entered or the memo can be sent via an email to the

supported email client, then copy the content of the email and paste the contents into the Memo, Tasks, or Notes application.

3.1 Datebook / Calendar entries / Memo entries

Datebook/calendar, Memo entries should contain various lengths of entries with various character sets (non-Latin characters) if supported.

- Long entry – over 160 characters or the maximum number of characters supported by the device
- Regular entry – normal length entry
- Entry without a title
- Special character entry – entry containing a special character e.g., *, !, &, %, $, @
- Deleted data – entries that have been deleted from the internal memory of the mobile device

4 Call Logs

The location of call log data will vary based upon make and model of mobile device. Typically, call log data may be viewed by pressing the talk button, which allows viewing a log of incoming, outgoing and missed calls. Additional data, such as the call date/time, and duration of the call can be viewed by selecting a specific call.

Call log data populated to the internal memory of a mobile device should contain different categories of calls i.e., incoming, outgoing and missed calls with the date/time of the call documented in addition to the duration of the call.

Populating the internal memory of the mobile device without service is limited to only outgoing calls, which will not be successful – due to lack of cellular service, but still present in mobile device memory.

Dependent upon the make and model of mobile device, Last Numbers Dialed (LND) from a supported (U)SIM or UICC may be transferred from the (U)SIM to the internal memory of the mobile device.

Populating the internal memory of a mobile device with cellular connectivity can be accomplished by, manually placing and receiving calls. The call type (i.e., incoming, outgoing, missed), date/time and duration of the call should be documented to determine that the mobile forensic application is properly reporting metadata for all call types.

5 SMS Messages

The make and model of mobile devices will determine how SMS messages are displayed. Some mobile devices when receiving a text message over 160 characters (often referred to as an SMS message) will display the message in multiple parts (i.e., individual messages) made up of 160 characters.

iOS mobile devices have two types of messages: regular text message and iMessages. When a text message is sent to a device that has an Apple ID, the Messages application automatically recognizes the owners Apple ID and routes the message through Apple's servers instead of using the cell phone carrier. iMessages typically have a blue background and the text entry field contains "iMessage" in the text entry field. Regular text messages for iOS devices are displayed with a green background and the text entry field contains "Text Message".

In order to verify mobile forensic applications are properly acquiring and reporting text messages and associated metadata, the internal memory should be populated with various categories of text messages. Testers should populate mobile devices with incoming, outgoing, drafts, iMessages (if supported), group messages (i.e., messages that contain more than one recipient) with varying lengths i.e., some messages should contain more than 160 characters. In addition to the type of message sent, the date/time stamp of when the message was sent/received should be documented.

Populating mobile devices lacking cellular service is limited to only outgoing SMS messages, which will be categorized as a draft. Dependent upon the make and model of mobile device, incoming text messages from a supported (U)SIM or UICC may be transferred from the (U)SIM to the internal memory of the mobile device.

Third party applications exist that allow the incoming and outgoing SMS messages to be sent and received over Wi-Fi. Dependent upon the operating system, make/model of the mobile device determines if third party text messaging applications can be installed.

Section 5.1 provides examples of data types for incoming, outgoing and draft messages (read, unread, deleted) that may be included when creating SMS text message data.

5.1 Incoming / Outgoing / Drafts

- Long entry – over 160 characters
- Regular entry – normal length entry
- Special character entry – contains special characters e.g., *, !, &, %, $, @
- Non-ASCII character entry – contains non-Latin characters
- Group messages – entry sent to multiple recipients
- Deleted data – messages that have been deleted from the internal memory of the mobile device

6 Multimedia Messaging Service (MMS) Messages

Similar to SMS textual based messages, the make and model of a mobile device will determine how MMS messages are transferred and displayed. MMS messages are messages that contain an attached graphic, video or audio file in addition to optional text message typed by the user.

The internal memory of populated mobile devices should contain various types of MMS messages. Testers should populate mobile devices with incoming, outgoing, drafts,

iMessages (if supported), group messages with varying text lengths. Each MMS message should contain an attached graphic, video or audio file. In addition to the type of message sent, the date/time stamp of when the message was sent/received should be documented.

Mobile devices lacking cellular connectivity are limited to outgoing MMS messages, which will be categorized as a draft. Third party applications exist that allow the incoming and outgoing MMS messages to be sent and received over Wi-Fi. Dependent upon the operating system, make/model of the mobile device determines if third party MMS messaging applications can be installed.

Sections 6.1 – 6.2 provide examples of data types that may be included when creating unread, read, and deleted MMS message data.

6.1 Incoming Picture, Audio, Video Messages

Require cellular connectivity or a third-party application must be installed on the mobile device (if supported) that allows MMS message data to be shared among devices connected over Wi-Fi. The textual portion of both incoming and outgoing MMS messages populated onto the internal memory of mobile devices should contain:

- Long entry – over 160 characters
- Regular entry – normal length entry
- Special character entry – contains special characters e.g., *, !, &, %, $, @
- Non-ASCII character contacts – contains non-Latin characters
- Group messages – entry sent to multiple recipients
- Deleted data – messages that have been deleted from the internal memory of the mobile device

6.2 Outgoing Picture, Audio, Video Messages

Outgoing picture, audio and video messages can be sent with or without cellular connectivity. For mobile devices lacking cellular connectivity, outgoing MMS data will be stored in the outgoing drafts of the internal memory of the mobile device. If the mobile device provides support for a third-party application, MMS message data can be shared among devices connected over Wi-Fi.

7 Stand-alone Files

Stand-alone supported files (i.e., graphic, audio, video) can be populated onto mobile devices with or without cellular connectivity. Various techniques exist for populating the internal memory of mobile devices with stand-alone (i.e., graphic, video, audio) files. Graphic, audio, and video files can be populated onto the internal memory of a mobile device using the device camera, video and audio recording facilities, if supported. This technique limits the tester to only one file format, as supported by the mobile device. Additional types stand-alone files should be populated onto the internal memory of the mobile device if supported. Examples of various file types are, graphic files (e.g., jpg,

gif, bmp, png), video (e.g., 3gp, mov, flv, avi, wmv), and audio (e.g., wav, aiff, mp3, flac, mp4).

Mobile devices with a service contract or cellular connectivity may be populated using the following techniques:

- Saving stand-alone file attachments (i.e., graphic, video, audio) that are stored on an email account, which the mobile device can access using a mobile email application.

- Bluetooth transfer – information between two devices can be shared over Bluetooth. This is dependent upon the make and model of the device and if Bluetooth transfers are supported. Bluetooth transfer allows data to be shared from one device to another by enabling and pairing two supported devices.

- PC synchronization software – data can be transferred to the mobile device if the device provides support and includes synchronization software. Individual files (i.e., graphic, video, audio) are transferred from a user's PC to the mobile device over a USB interface.

8 Application Related Data

Dependent upon the make and model of mobile device determines the native applications available. Native applications may include apps allowing users to create documents, spreadsheets, slide shows, databases, etc. Data can be populated onto the internal memory of mobile devices supporting various applications with or without cellular connectivity. The types of application related data populated onto the mobile device is based upon the operating system and make/model of the mobile device.

9 Internet Related Data

Internet related data can be populated onto mobile devices that either possess cellular connectivity or Wi-Fi capabilities. Depending on the operating system, make/model of the mobile device will determine the browser (e.g., Chrome, Safari) support provided natively by the mobile device.

Internet history, bookmarks and login information to a specific account/accounts are populated onto the internal memory of the mobile device by the following actions (each of which must be documented):

- Visiting various web sites by opening the mobile device browser and inputting the URL of interest
- Bookmarking various sites of interest
- Successfully logging in to email accounts (e.g., gmail, Yahoo)

10 Social Media Related Data

Social media related data can be populated onto mobile devices with network connectivity. Many smartphones come pre-loaded with various social media applications such as: Facebook, LinkedIn, Twitter, etc. Social media applications allow individuals to share status information, pictures and personal message (PMs).

For mobile devices that do not come pre-loaded with social media applications, testers minimally should install Facebook, Twitter and LinkedIn for supported mobile devices. Individual social media accounts can either be created from a personal computer with network access or directly from the mobile device.

When populating the internal memory of mobile devices that support various social media applications it is advantageous to create two social media accounts (e.g., mobile_1, mobile_2). The creation of two accounts across the installed social media applications (e.g., Facebook, LinkedIn, Twitter) enables the user to maintain control over the personal messages shared between accounts, status updates, in addition to populating profile pictures, albums, sharing videos, etc.

Social media accounts used to populate the internal memory of mobile devices should at a minimum include the following: Profile pictures, profile information (high school, college, employer, current city, hometown), picture albums, personal messages shared between mobile_1 and mobile_2 accounts.

Dependent upon the social media application determines the richness of data that users can create and share between accounts. Typically, each application provides users with the ability to provide a profile (picture, background information) of the account and the ability to share status information that may or may not include pictures, video or audio files.

11 GPS Related Data

Dependent upon the make and model of mobile device determines if and how much GPS related data (waypoints, longitude and latitude coordinates) can be populated onto the internal memory of the device. When populating GPS related data (e.g., waypoints, geotagging, checking-in) on mobile devices the locations services must be activated. The location service is typically located within the Settings menu for most mobile devices.

GPS coordinates associated with routes, geotagged pictures and videos, “checking-in” via social media applications can be populated onto mobile devices through network connectivity. In order to populate GPS route data (waypoints), it is helpful if the mobile device has cellular connectivity. Although dependent upon the strength and coverage of wireless connectivity over Wi-Fi, users may be able to start a route at one point and travel to another location within the wireless coverage range.

Geotagging pictures and videos or “checking-in” using social media applications can be accomplished if the mobile device is able to establish cellular or Wi-Fi connectivity.

Geotagging is typically enabled beneath the camera icon security settings. Geotagged pictures and videos provide longitude and latitude coordinates for where the picture or video was taken. Another popular social media functionality is allowing users to share their current location, otherwise known as "checking-in". Checking-in provides users with the ability to share their current location at a specific date and time through their social media status. Checking-in is typically a setting that is enabled through social media security settings.

Appendix A – Mobile Device Population Data Example

Appendix A – contains an example/template of a dataset used for populating the internal memory of a mobile device. The format contains data element categories and sub-categories within each root data element.

Handset Internal Memory:

<Address Book>

<Long Name (50 chars), Mobile Number>

John Jacob Jingle Heimer Schmidt That's My Name Too Whenever I Go Out The People Always Shout John Jacob Jingle Heimer Schmidt

, 8988675309

<Regular Name, Mobile Number, email, website, picture>

Jimi Hendrix, 7691234560, hendrix@experienced.com, website: www.jimihendrix.com

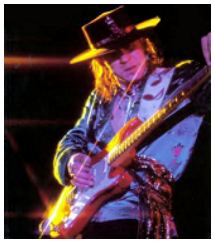
<Special Character Name, Home Number>

*, 8887771212

<Blank Name, Work Number>

, 8785551111

*<Regular Name, Mobile Number, email, deleted picture, address, birthday>*Stevie Ray Vaughn, 1234567890, work: stevie@srv.com, address: 1234 Main Street, Dallas, TX, SRV Birthday: October 3, 1954,



<Deleted Entry, Home Number >

John Bonham, 9878767654

<Non-ASCII Entry, Mobile Number>

阿□哈拉, +86 35 8 763 30 07

<Non-ASCII Entry, Number>

Aurélien, +33 22 6 555 20 20

<Groups contact entry >

27 Club: Jimi Hendrix*, Stevie Ray Vaughn*, John Bonham

Note: the contact entries within the Group contain data consistent as displayed above.

<PIM Data>

<Datebook/Calendar>

<Long Title (160 chars), Date: 3-03-16, Type: Reminder>

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!!

<Regular Title, Date: 4-23-16, 6am, Location: Los Angeles Type: Meeting>

Rush concert

<Deleted Entry, Date: 9-16-16, Type: Memo>

Hendrix summer of love documentary

<Entry without Title, Date: 10-10-16, Type: Reminder>

<Special Char Entry, Date: 12-21-16, Type: Reminder>

!

<Memo>

<Long Memo (3000 chars)>

The goal of the CFTT project at NIST is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities. NIJ has published test reports on several forensic imaging tools, several software write block tools and a variety of hardware write block devices. Currently specifications and test methodologies for deleted file recovery and string searching tools are in development. In addition to forensic tools for acquisition and analysis of digital data on desktop and laptop computers, CFTT is also developing test methodologies for mobile devices. Data acquisition performed on cellular devices operating over Global System for Mobile Communications and non-GSM networks has proven not only frustrating but extremely tedious due to the rapid rate of new cellular devices available on the market. Software vendors specializing in cellular forensics are forced to continuously provide updates to software and associated hardware in order to maintain support and provide examiners with solutions for the latest technologies. Mobile device forensic research performed at the NIST ITL has produced numerous reports on tools capable of acquiring data from Personal Digital Assistants, smart phones, and cellular devices operating over GSM and non-GSM networks. NIST has presented to numerous conferences world-wide providing software vendors, forensic specialists, incident response team members, and law enforcement an overview of the current capabilities and limitations of forensic applications capable of acquiring data from cellular devices as well as suggestions on preservation and handling of digital data. Research conducted over the past two years has produced the following publications: NISTIR 7250 Cell Phone Forensic Tools: An Overview and Analysis, SP800-101 Guidelines on Cell Phone Forensics, NISTIR 7387 Cell Phone Forensic Tools: An Overview and Analysis Update, Forensic Software Tools for Cell Phone Subscriber Identity Modules. In addition to the NIST reports and conference articles produced our research has provided extensive involvement with software engineers from various manufacturers troubleshooting potential issues, providing suggestions on product improvement and overall dependability, which have played a key role in the evolution of cellular forensics software. Research conducted and shared materials have shown to be invaluable insofar as providing academia with a starting point for education materials, informing law enforcement and forensic examiners of expectations of the interaction between numerous devices and tools, and informing vendors of anomalies while providing a baseline for software improvement.

<Short Memo>

This is a short active memo entry.

<Deleted Memo>

This entry has been deleted from the memo application.

<Call Logs>

<Missed Calls, non-deleted>

301642xxxx

<Missed Calls, deleted>

301975xxxx

<*Incoming, non-deleted***>**

301975xxxx

<*Incoming, deleted*>

301642xxxx

<*Outgoing, non-deleted*>

301642xxxx

<Outgoing, deleted>

301975xxxx

<Incoming SMS Messages>

<*Message, status: read***>**

The following SMS message is a read incoming message sent from another device

<*Message, status: unread***>**

The following SMS message is an unread incoming message sent from another device

<*Deleted message*>

This is a deleted incoming message sent from another device

<*Message, status: read, 160 chars***>**

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.

<*Message, status: unread, 160 chars***>**

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.

<*Deleted message*>

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.

<Outgoing SMS Messages>

<Message, status: active >

The following SMS message is an active outgoing message sent to another device

<Message, group >

The following SMS message is an active outgoing group message sent to multiple recipients

<Deleted message>

This is a deleted outgoing message sent to another device

<Message, status: active, 160 chars>

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.

<Message, group 160 chars>

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.

<Deleted message>

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.

<Incoming MMS Messages>

<Message, Audio, read>

Incoming sound byte MMS message contains the following,
Audio: *Today's Date is: Day, Date, Year*

<Message, Image, unread>

Incoming image mms message contains a picture of today's date,
Image: *date*

<Message, Video, read>

Incoming video message

<Outgoing MMS Messages>

<*Message, Audio* >

Outgoing sound byte message contains audio of the current date

Message description:

Audio: *Outgoing sound byte message today's date is: day, date, year*

<*Message, Image* >

Outgoing image MMS message contains a picture of the current date

<*Message, Video* >

Outgoing video message contains video of the current date

<Stand-alone Data Files>

<*Audio*>

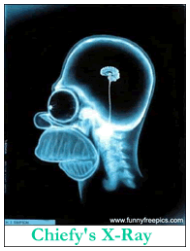
wav file uploaded to the mobile device

<*Deleted audio*>

mp3 file uploaded to the mobile device

<Active *Images*>

 emma-girl.jpg



homer.gif

<*deleted image*>

 winter.bmp

<Documents>

<deleted text file> Gibson.txt

Gibson USA 2004 models: Les Paul, SG, X-Factor, Voodoo, Chet Atkins, Faded, Bass, Americana

<pdf file> forensics.pdf
Forensics is an emerging technology that is branching off into many different avenues (e.g., PDA Forensics, Cell Phone Forensics, Network Forensics, and Stand Alone machine Forensics.

<*video*>

mp4 video file uploaded to the mobile device

<*deleted video*>

mp4 video file uploaded to the mobile device

<Internet Data>

<*Visited Sites*>

www.nist.gov

www.mobileforensicsworld.org

www.computerforensics.com

<*Bookmarked Sites*>

www.cftt.nist.gov

www.cfreds.nist.gov

www.phonescoop .com (deleted)

<*Additional Sites* >

www.gmail.com

www.facebook.com

www.twitter.com

www.linkedin.com

login: account1@email.com, account2@email.com

<Email Data>

From: account1
Subject: Photos
Body: The following email contains graphic files. (three attachments)

From: account1
Subject: long memo
Body: The goal of the CFTT project at NIST is...

From: account1
Subject: video
Attachment: video.mp4

From: account1
Subject: audio file
Attachment: audio.wav

From: account1
Subject: audio file
Attachment: audio.mp3

From: account1
Subject: document.pdf
Attachment: document.pdf

From: account1
Subject: document.txt
Attachment: document.txt

<GPS Data >

Current location
Turn on Geo-tagging and take various pictures and video.
Document location and which pictures, videos contain geotag information.

<**Social Media Data**>
<Facebook>

Account: account1 (John Doe), account2 (Jane Doe)
Profile pic, 3 albums (pics in each), chat logs, wall posts, profile info, video

Account1 – (John Doe)

profile pic:

cover pic: 

profile info:

High School: High School 1
College/University: Rhoads University
Employer: TSIN
Current City: House of TTFC
Hometown: City of Angels

Albums: Camaro Pics, Weather Pics, Mobile Uploads
Pics uploaded from phone (Mobile Uploads)-

Chat – account1 to account2: Hello account2, nice pictures account2.

Account1 to account2: This is a deleted Facebook message to determine if tools are able to recover any data remnants.

<Twitter>

Account: account1, account2
Fill out profile information and follow each other, post tweets
Note: account1 and accoutn2 follow each other.

Account1 (tweet): account1 is feeling slightly digital today and needing to tweet a pic.

Personal Message to account2: Hello @account2, thanks for the follow on twitter.

Account2 to account1 (message): Good morning @account1, thank you for the follow back!

<LinkedIn>

Account: account1, account2

Profile info:
John Doe, Jane Doe – Computer Scientist at TSIN, Gaithersburg, MD – Research

Account1 and account2 are connections on linkedin.

Account1 message to account2:
Hi Jane – thank you for the connection on Linkedin. Hope all is well.

Account2 reply: Hello John – likewise.

<Instagram>

Account: account1
Profile info
Profile picture

Name: account1 name
Email: account1@email.com
Username: account1
Phone Number: 5551212
Sex: male
Bio: short bio for account1
Website: account1@account1.com

Site contains various photos and video