Appendix A – Mobile Device Population Data

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.

MOTO-E
IMEI: 990005f455781717
MEID: 99000545578171
ICCID: 89148000002239843599

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>
阿恶哈拉, +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
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>
<Outgoing, non-deleted>
3019754871
<Outgoing, deleted>
2402528734

<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.
<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

<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>

Whitehouse Washington DC
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 account2 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>
  Was logged on from Internet – app not installed
  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.


<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