Collaborative Testing Services, Inc.
FORENSIC TESTING PROGRAM

P.O. Box 650820 Sterling, VA 20165-0820
e-mail: forensics@cts-interlab.com
Telephone: +1-571-434-1925
Fax: +1-571-434-1937

Manufacturer's Information

Mobile Digital Evidence Test No. 17-5550

The Mobile Digital Evidence sample set consisted of data acquired from a smart phone in .BIN and .DD file formats. Participants were asked to examine the extracted data pertaining to a simulated scenario utilizing their own software and methods.

SAMPLE PREPARATION:
The phone data was generated following a scripted scenario based upon a phone that was recovered at the scene of a crime. The script was planned and executed during the week of February 27, 2017. An LG MS428 K10 smart phone was used to perform the scripted activities to generate the intended artifacts.

The phone data was acquired through a physical extraction of the LG MS428 K10 smart phone utilizing Cellebrite software. Following sample validation, the phone data was converted into .BIN and .DD compressed archive files. These files were uploaded to the CTS portal for participants to download. MD5 and SHA-1 algorithms were run on the compressed archives to generate unique hash values to allow participants to validate the successful download of the files.

SAMPLE VALIDATION/VERIFICATION:
The validation stage consisted of the examination of the phone data utilizing various software to ensure expected results could be achieved. Laboratories that conducted predistribution results of the sample data reported consistent results.

PLEASE NOTE: Questions marked with asterisks (**) did not show a clear consensus during preliminary review of the participants' responses. Further information and discussion will be available in the final report.

SCENARIO PROVIDED TO PARTICIPANTS:

On March 3, 2017, a witness found a body at Bull Run Regional Park in Centerville, Virginia and notified local police. Upon their arrival, police identified the body to be Nicole Cooper who was reported as missing. While investigating the area, police discovered an abandoned LG MS428 K10 smart phone that was collected for evidence. After logging the phone into evidence, a physical image of the smart phone was created. You have been tasked with analyzing the physical image of the smart phone utilizing your own tools and methods to determine if this device has relevance to the investigation.

The information presented here details how test samples were prepared as well as any design specifications. This information does not necessarily represent the answers that should or could be obtained from an examination of the sample(s). Final interpretation of the results should be deferred until the summary report is available.

Question	*Manufacturer's Expected Response*
1	Provide the MD5 hash value for the decompressed image file. *6c17d83b5134cdb5f069db9104658a41*
2	Provide the SHA1 (base 16) hash value for the decompressed image file. *10abbf12a9d47fc6f608da9336d7b97c2e1ed08a*
3	What is the phone number associated with this device? *571-758-0731*
4	Which phone vendor is associated with this device? *MetroPCS*
5	What is the set time zone for this device? *America/New_York*
6	Provide the city/state this device was set to per the LG weather services database. *Herndon/Virginia*
7	What is the Google e-mail account associated with this device? *bencooper1381@gmail.com*
8	As per the Bluetooth configuration file, this device was connected to a vehicle. Provide the vehicle name this device was connected to as mentioned in this file. *Santa Fe Sport*
9	As per the Bluetooth configuration file, provide the EPOCH timestamp value for when this device first connected to the vehicle. *1488393923*
10	Convert the EPOCH timestamp value of when this device first connected to the vehicle in USA/Canada Eastern Time with the following format: Month/Day/Year, Hours:Minutes:Seconds AM/PM. *3/1/2017, 1:45:23 PM*
11	How many wireless networks was this device connected to? *Three (3)*
12	What is the PSK (password) value for the B21-Guest network? *bwireless*

Question	*Manufacturer's Expected Response*
13	What terms were searched in the Google Play Store? *pof, facebook messenger*
14	What third-party application was downloaded first on this device? *PoF Free Dating App*
15	What is the package_name for the Waze Application? *com.waze*
16	Provide the POF Free Dating Application username associated with this device. *bcooper1381*
17	Via the POF Free Dating Application, provide the username whose sender_profile_id is 139693337. *laurelmurray*
18**	How many URLS were visited in Chrome? *Twelve (12)*
19	What is the title of the last website visited in Google Chrome? *10 Ways To Dispose Of A Dead Body (If You Really Needed To)*
20	How many calendar events are listed on this device? *Four (4)*
21	Provide the calendar event names listed in the calendar database. *Nicole's Birthday, Jack's Birthday, Doctor Smith, Hike at Balls Bluff Regional Park - Leesburg*
22	What are the memos (names) of the alarms that were named? *Wake up for work, Feed Jack*
23	How many locations were visited via Waze? *Three (3)*
24	Provide the location names visited via Waze from the "Recents" table. *Claude Moore Park, Ball's Bluff Battlefield Regional Park, Bull Run Regional Park*
25	Provide the name of the last location this device traveled to via Waze from the "Recents" table. *Bull Run Regional Park*

Question	*Manufacturer's Expected Response*
26	Provide the EPOCH timestamp value for the last location visited in Waze. *1488554764*
27	Convert the EPOCH timestamp value of the last location in Waze was visited in US/Canada Eastern Time with the following format: Month/Day/Year, Hours:Minutes:Seconds AM/PM. *3/3/2017, 10:26:04 AM*
28	Provide the coordinates for the last location this device traveled to via Waze. Answer must be recorded as (Latitude, Longitude). *(38802055, -77491301)*
29	How many MMS messages were sent to this device? *Two (2)*
30	What is the contact name for 202-749-9211? *Laurel Murray*
31	How many outgoing phone calls are to 202-749-9211 which lasted greater than 1 minute? *Two (2)*
32	How many voicemails are from 202-749-9211? *Four (4)*
33	Provide the EPOCH timestamp value of when the first voicemail was received on this device. *1488288430000*
34	Convert the EPOCH timestamp value of when the first voicemail was received on this device in US/Eastern Standard time with the following format: Month/Day/Year, Hours:Minutes:Seconds AM/PM. *2/28/2017, 8:27:10 AM*
35	How many SMS messages are FROM 202-749-9211? *Fourteen (14)*
36	How many SMS messages were SENT to 202-749-9211? *Fifteen (15)*
37	Provide the body of the SMS message for the EPOCH time stamp value of 1488472825463. *A hammer, duct tape, and a tarp.*

Question	*Manufacturer's Expected Response*
38**	An MMS message was received from 202-749-9211 with a receipt for the purchased items. What is the date and time on the receipt of when these items were purchased? Report date and time exactly as shown. *03/02/17 01:58 PM*
39	What is the name of the attachment sent in the MMS message which contained the receipt of the purchased items? *image000000(1).jpg*
40	What is the body of the last SMS message RECEIVED from 202-749-9211? *But Ben, you're going to end up in jail!*
41	What is the EPOCH timestamp value of the last SMS message SENT to 202-749-9211? *1488557347348*
42	Convert the EPOCH timestamp value of the last SMS message SENT to 202-749-9211 in US/Canada Eastern Time with the following format: Month/Day/Year, Hours:Minutes:Seconds AM/PM. *3/3/2017, 11:09:07 AM*
43	What is the body of the last SMS message SENT to 202-749-9211? *No I'm not! I know what I'm doing!*
44	How many e-mails were received from nicolecooper23@aol.com? *Eight (8)*
45	How many e-mails were sent to nicolecooper23@aol.com? Do NOT include e-mails that were deleted. *Eight (8)*
46	Provide the subject field of the first received e-mail from nicolecooper23@aol.com on March 2, 2017. *Divorce*
47	Provide the EPOCH timestamp value for the last e-mail sent to nicolecooper23@aol.com. *1488487973000*
48	Convert the EPOCH timestamp value for the last e-mail sent to nicolecooper23@aol.com in US/Eastern Time with the following format: Month/Day/Year, Hours:Minutes:Seconds AM/PM. *3/2/2017, 3:52:53 PM*
49	What is the subject field of the last e-mail sent to nicolecooper23@aol.com? *Talk tomorrow*

Question	*Manufacturer's Expected Response*
50 What is the body of the last e-mail sent to nicolecooper23@aol.com?	*Nicole, Let's meet tomorrow and discuss our relationship. We can go for a walk at Bull Run Park in Centerville. Meet me there at 11 AM. Ben*
51 At the conclusion of your analysis, who does this device belong to?	*Ben Cooper*
52 Does this device have relevance to the investigation? (Yes/No)	*Yes*