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 or
Toll-free Fax (US only): 1-866-fax-2cts

Manufacturer's Information

Mobile Digital Evidence Test No. 15-5550

The Mobile Device Examination test consisted of sample data that was extracted from a smartphone. The sample data included one data partition (userdata.dd); stored in the .dd format. Participants were asked to examine the provided sample data utilizing their own tools and methods.

SAMPLE PREPARATION
The sample data was generated following a scripted scenario. The scenario was based upon an identity theft scam planned and executed in December of 2014. The suspect's phone (Samsung Galaxy S III (SCH-R530C)) was used to perform the scripted activities in order to generate the intended data artifacts.

The sample data was obtained from the suspect's phone using AccessData's Mobile Phone Examiner Plus (MPE+). Following all necessary steps outlined in MPE+, a physical extraction was conducted on the suspect's phone.

Following sample validation, the sample data was compressed into a .rar data archive. MD5 and SHA1 hash algorithms were run on the data archive to generate unique hash values. The data archive, and the associated hash values, were uploaded to the CTS portal for participants to download.

SAMPLE VALIDATION/VERIFICATION
The validation stage consisted of the examination of the sample data utilizing various different tools to ensure that all expected responses could be achieved. Laboratories that conducted predistribution analysis of the sample data reported consistent results.

PLEASE NOTE: Questions marked with an asterisk "*" did not show a clear consensus during preliminary review of participant responses. Further information and discussion will be available with the final report.

UPDATE (9/10/15): Question 15 and 38's expected manufacture's response have been updated from the original MI.

SCENARIO PROVIDED TO PARTICIPANTS
Police are investigating a case of attempted identity theft. On December 12th, Harris Marvins contacted the local police department claiming that someone tried to take out a loan in his name. Mr. Marvins reported that suspect Steven Lefft convinced him that he had come into a large inheritance from a long lost relative in Africa. After some communication and information exchange with Mr. Lefft, Mr. Marvins was instructed to wait to receive legal documents in the mail. Mr. Marvins reported receiving notice from his local bank that a request for a home loan had been made in his name. Acting quickly, Mr. Marvins reported this information to the police. On December 13th, the police executed a search warrant at the residence of Mr. Lefft. During the search, police seized a Samsung Galaxy S III (SCH-R530C) smartphone. The police took the seized smartphone back to headquarters and performed a physical extraction using AccessData's Mobile Phone Examiner Plus. The police are requesting that you examine the extracted data partition (.dd format) and identify any information that can implicate Mr. Lefft in this crime, determine if he was working with any co-conspirators, and uncover any other scams that Mr. Lefft may be involved with.

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 userdata.dd partition. *930d723822ae61294c1252bd06c2a663*
2	Provide the SHA1 hash value for the userdata.dd partition. *27ffda23c0f8a77844d4d7613f291fe261c49483*
3	What is the device name as reported in the android providers' settings? *SCH-R530C*
4	What is the Bluetooth address for the phone? *94:01:C2:2F:94:FC*
5	What time zone is the phone configured for? (Provide the answer as GMT +/- hours) *GMT -5*
6	What city was the phone located in when it was last turned on? (As provided in the android providers' settings) *Cascades*
7	What is the active Gmail account on the phone? *lefty21331@gmail.com*
8	What was the last application that the suspect Steven Lefft downloaded? (Provide the application's package name) *com.konylabs.capitalone*
9	Did the suspect Steven Lefft add the victim Harris Marvins as a contact in his phone book? *Yes*
10	The suspect Steven Lefft connected to a wireless network with the SSID "HideoutHotspot". What was the password for this wireless network? *123steal*
11	The suspect Steven Lefft attempted to connect with another phone via Bluetooth. What is the name of the phone that he tried to connect to? *dadami's iPhone*
12	When was the Viber app last launched? (Present date in dd-mm-yyyy format and present time in hh:mm:ss adjusted for the phone's local time zone in 24 hour format)* *11-12-2014 15:53:18*

Question	*Manufacturer's Expected Response*
13	The suspect Steven Lefft copied a phone number to his clipboard, what was the phone number? (Provide the number as it is displayed) *5712129673*
14	What terms did the suspect Steven Lefft search in the Google Play store? *email, viber, banks*
15	Provide the coordinates where the picture "20141211_141619.jpg" was taken? (Format exactly as displayed in the EXIF data)* *Latitude 39" 1' 31.952* *Longitude 77" 24' 7.328*
16	In Facebook Messenger, the suspect Steven Lefft sent Paul one message. Provide the coordinates associated with this message.* *latitude:39.030476* *longitude:-77.40115*
17	The suspect Steven Lefft created a fake Facebook profile. What was the name of the Facebook profile? *Anwar Mogba*
18	What display phone number did the suspect Steven Lefft use to register with the Facebook application? (###) ###-#### *(443)518-0022*
19	What email address did the suspect Steven Lefft use to register on Facebook? *leftout21331@yahoo.com*
20	What is the suspect Steven Lefft's one Facebook friend's display name? *Paul Gee*
21	What did the suspect Steven Lefft search using Google? (Duplicate searches only need to be reported once) *fraud, vacation homes*
22	In Chrome, what is the url of the first web page that the suspect Steven Lefft visited? *http://www.justice.gov/criminal/fraud/websites/idtheft.html*
23	In Chrome, the suspect Steven Lefft visited the Department of Justice's web page (US DOJ). When did he visit this web page? (Based off of last visit time) (Present date in dd-mm-yyyy format and present time in hh:mm:ss adjusted for the phone's local time zone in 24 hour format) *11-12-2014 10:24:42*

Question	***Manufacturer's Expected Response***
24	In Google maps the suspect Steven Lefft requested driving directions to a bank. Provide the name of the bank. *Capital One Bank*
25	The suspect Steven Lefft created an Outlook email account. What is the name associated with that account? *Fund Scam*
26	What email address was used in the Outlook app? *Inheritancefoundation21331@outlook.com*
27	What is the victim Harris Marvins' email address? *harris.marvins@aol.com*
28	What is the subject of the email conversation between the suspect Steven Lefft and the victim Harris Marvins? *Inheritance*
29	In the email conversation, the victim Harris Marvins sent the suspect Steven Lefft an attachment. What is the name of the attachment? *SS.png*
30	The suspect Steven Lefft sent emails through the Outlook app to the victim Harris Marvins. In one of the emails Mr. Lefft tells Mr. Marvins about the estimated value of his cousin's estate. How much was the estate valued at? *$50 million dollars*
31	Did the suspect Steven Lefft ever text message the victim Harris Marvins? *Yes*
32	What is the filename of the attachment that the suspect Steven Lefft sent Paul through text message? *20141211_140829.jpeg*
33	When did the suspect Steven Lefft first call Paul? (Using the phone, not a 3rd party calling application) (Present date in dd-mm-yyyy format and present time in hh:mm:ss adjusted for the phone's local time zone in 24 hour format)* *10-12-2014 11:02:31*
34	The suspect Steven Lefft had a missed call from the victim Harris Marvins. When did this call attempt occur? (Present date in dd-mm-yyyy format and present time in hh:mm:ss adjusted for the phone's local time zone in 24 hour format)* *11-12-2014 10:43:40*
35	What is the content of the last text message that the suspect Steven Lefft sent to Paul? *Of course I did. We're gonna be rich brother!*

Question	*Manufacturer's Expected Response*
36 How many Viber calls occurred between the suspect Steven Lefft and Paul? (Include calls with 0 duration)*	*5*
37 When did the last Viber call between the suspect Steven Lefft and Paul take place? (Present date in dd-mm-yyyy format and present time in hh:mm:ss adjusted for the phone's local time zone in 24 hour format)*	*11-12-2014 15:53:28*
38 What is the last message that the suspect Steven Lefft sent to Paul in the Viber app.*	*Pretty good sounds quality*
39 The suspect Steven Lefft received a text message from Paul identifying a new target for their next scam. What is the name of the person that Paul provided to Mr. Lefft?	*George Trews*