Collaborative Testing Services, Inc
FORENSIC TESTING PROGRAM

Mobile Device Examination Research Test No. 15-5550 Summary Report

This test was provided to 52 participants. Participants were provided the data yielded from a physical extraction of the suspect phone. They were asked to examine the provided sample data utilizing their own tools, and methods, and answer scenario specific questions. Data were returned from 32 participants (61.5% response rate) and are compiled into the following tables:

	Page
Manufacturer's Information	2
Summary Comments	6
Table 1: Digital Evidence Responses	7
Table 2: Additional Comments	85

This report contains the data received from the participants in this test. Since these participants are located in many countries around the world, and it is their option how the samples are to be used (e.g., training exercise, known or blind proficiency testing, research and development of new techniques, etc.), the results compiled in the Summary Report are not intended to be an overview of the quality of work performed in the profession and cannot be interpreted as such. The Summary Comments are included for the benefit of participants to assist with maintaining or enhancing the quality of their results. These comments are not intended to reflect the general state of the art within the profession.

Participant results are reported using a randomly assigned "WebCode". This code maintains participant's anonymity, provides linking of the various report

Manufacturer's Information

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.

Manufacturer's Information, continued

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

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

Manufacturer's Information, continued

Question ***Manufacturer's Expected Response***

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

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

Manufacturer's Information, continued

Question ***Manufacturer's Expected Response***

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!

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

Summary Comments

Participants were provided data yielded from a physical extraction of the test phone, along with a scenario detailing the sample data. The sample data included one partition in .dd format. Participants were asked to examine the provided sample data utilizing their own tools, and methods, and answer scenario specific questions.

The focus of this test was to prompt participants to examine different data artifacts generated from a suspect's recovered phone. Participants were requested to analyze artifacts addressing common examination areas such as: SMS/MMS, call logs, e-mail, Geo-location information, web browsers, and application use. Test questions were designed to be tool neutral, however, in some instances, this required participants to perform manual examination of the data artifact in question.

Consensus was achieved for the majority of the questions asked. However, ten of the questions did not reach a consensus. Five of these questions (12, 23, 33, 34, and 37) dealt with date and time conversion issues. Two of the questions (15 and 16) dealt with latitude and longitude issues. Three of the questions (6, 36, and 38) dealt with issues about the question asked. In future iterations of the test we will be addressing some of the feedback provided by participants to improve the test. Improvements will be made to clarity of question and requested answer formats. This should help produce more consistent responses with regard to conversions.

Digital Evidence Responses

TABLE 1

Question 1 - Image Details

Question 1: Provide the MD5 hash value for the userdata.dd partition.

Manufacturer's Expected Response: 930d723822ae61294c1252bd06c2a663

WebCode	Response
2HZNCM	930d723822ae61294c1252bd06c2a663
2MX9EK	930d723822ae61294c1252bd06c2a663
2W2HLB	930D723822AE61294C1252BD06C2A663
3JPC9M	930d723822ae61294c1252bd06c2a663
3UP3RA	930D723822AE61294C1252BD06C2A663
6GECZL	930d723822ae61294c1252bd06c2a663
6HAU49	930d723822ae61294c1252bd06c2a663
7TLJFH	930d723822ae61294c1252bd06c2a663
9MAA37	930d723822ae61294c1252bd06c2a663
ATTZ37	930d723822ae61294c1252bd06c2a663
BDWZNC	930d723822ae61294c1252bd06c2a663
EXQ8BW	930D723822AE61294C1252BD06C2A663
EZFET9	A8116FE3DA2F57B7FE9F90863ADB351B
FFMX46	930d723822ae61294c1252bd06c2a663
FHB8E7	930d723822ae61294c1252bd06c2a663
H46R9T	930D723822AE61294C1252BD06C2A663
H47R79	930D723822AE61294C1252BD06C2A663
JVM7CV	578E368B3BF4173D61FD9D045C744293
LHAK2Z	930d723822ae61294c1252bd06c2a663
LJ7ZDX	930D723822AE61294C1252BD06C2A663
NQYVN2	930D723822AE61294C1252BD06C2A663
R6PT4T	930d723822ae61294c1252bd06c2a663
RECRVY	930d723822ae61294c1252bd06c2a663
RY2BNW	930d723822ae61294c1252bd06c2a663
RYWRZT	930d723822ae61294c1252bd06c2a663
TCHNEW	930d723822ae61294c1252bd06c2a663
UCCT9V	930d723822ae61294c1252bd06c2a663
UD8CCH	930d723822ae61294c1252bd06c2a663
ULK4ZV	930d723822ae61294c1252bd06c2a663
WLY9DQ	930d723822ae61294c1252bd06c2a663
XPRVJJ	930d723822ae61294c1252bd06c2a663
ZYQ8TH	930d723822ae61294c1252bd06c2a663

TABLE 1

Question 1 - Image Details

Consensus Result: 930d723822ae61294c1252bd06c2a663

Expected Response Explanation:

This hash value can be achieved by decompressing the supplied .zip file and running a MD5 hash algorithm on the 15-5550userdata.dd partition.

TABLE 1

Question 2 - Image Details

Question 2: Provide the SHA1 hash value for the userdata.dd partition.

Manufacturer's Expected Response: 27ffda23c0f8a77844d4d7613f291fe261c49483

WebCode	Response
2HZNCM	27ffda23c0f8a77844d4d7613f291fe261c49483
2MX9EK	27ffda23c0f8a77844d4d7613f291fe261c49483
2W2HLB	27FFDA23C0F8A77844D4D7613F291FE261C49483 base16 E775UI6A7CTXQRGU25QT6KI74JQ4JFED base32
3JPC9M	27ffda23c0f8a77844d4d7613f291fe261c49483
3UP3RA	E775UI6A7CTXQRGU25QT6KI74JQ4JFED
6GECZL	27ffda23c0f8a77844d4d7613f291fe261c49483
6HAU49	27ffda23c0f8a77844d4d7613f291fe261c49483
7TLJFH	27ffda23c0f8a77844d4d7613f291fe261c49483
9MAA37	27ffda23c0f8a77844d4d7613f291fe261c49483
ATTZ37	27ffda23c0f8a77844d4d7613f291fe261c49483
BDWZNC	27ffda23c0f8a77844d4d7613f291fe261c49483
EXQ8BW	E775UI6A7CTXQRGU25QT6KI74JQ4JFED
EZFET9	B7C64021DE09375E24ED26F073129D39DED85E4F
FFMX46	27ffda23c0f8a77844d4d7613f291fe261c49483
FHB8E7	27ffda23c0f8a77844d4d7613f291fe261c49483
H46R9T	27FFDA23C0F8A77844D4D7613F291FE261C49483
H47R79	27FFDA23C0F8A77844D4D7613F291FE261C49483
JVM7CV	34BA4AAA439972A90EBC4269DCF7586B5BAF5E79
LHAK2Z	27ffda23c0f8a77844d4d7613f291fe261c49483
LJ7ZDX	27FFDA23C0F8A77844D4D7613F291FE261C49483
NQYVN2	27FFDA23C0F8A77844D4D7613F291FE261C49483
R6PT4T	27ffda23c0f8a77844d4d7613f291fe261c49483
RECRVY	27ffda23c0f8a77844d4d7613f291fe261c49483
RY2BNW	27ffda23c0f8a77844d4d7613f291fe261c49483
RYWRZT	27ffda23c0f8a77844d4d7613f291fe261c49483
TCHNEW	27ffda23c0f8a77844d4d7613f291fe261c49483
UCCT9V	27ffda23c0f8a77844d4d7613f291fe261c49483
UD8CCH	27ffda23c0f8a77844d4d7613f291fe261c49483
ULK4ZV	27ffda23c0f8a77844d4d7613f291fe261c49483
WLY9DQ	27ffda23c0f8a77844d4d7613f291fe261c49483
XPRVJJ	27ffda23c0f8a77844d4d7613f291fe261c49483
ZYQ8TH	27ffda23c0f8a77844d4d7613f291fe261c49483

TABLE 1

Question 2 - Image Details

Consensus Result: 27ffda23c0f8a77844d4d7613f291fe261c49483

Expected Response Explanation:

This hash value can be achieved by decompressing the supplied .zip file and running a SHA1 base 16 hash algorithm on the 15-5550userdata.dd partition.

Other Responses:

Three participants reported the SHA1 hash base 32 (E775UI6A7CTXQRGU25QT6KI74JQ4JFED) as a response. This response was not highlighted as the question did not specify which SHA1 hash was expected.

TABLE 1

Question 3 - Phone settings

Question 3: What is the device name as reported in the android providers' settings?

Manufacturer's Expected Response: SCH-R530C

WebCode	Response
2HZNCM	SCH-R530C
2MX9EK	SCH-R530C
2W2HLB	SCH-R530C
3JPC9M	SCH-R530C
3UP3RA	SCH-R530C
6GECZL	Samsung SCH-R530 Galaxy S III LTE
6HAU49	SCH-R530C
7TLJFH	SCH-R530C
9MAA37	SCH-R530C
ATTZ37	SCh-R530C
BDWZNC	SCH-R530C
EXQ8BW	SCH-R530C
EZFET9	SCH-R530C
FFMX46	SCH-R530C
FHB8E7	SCH-R530C
H46R9T	Steve Lefft
H47R79	SCH-R530C
JVM7CV	556e2f1b16bf5efa
LHAK2Z	SCH-R530C
LJ7ZDX	SCH-R530C
NQYVN2	SCH-R530C
R6PT4T	SCH-R530C
RECRVY	SCH-R530C
RY2BNW	SCH-R530C
RYWRZT	Steve Lefft
TCHNEW	SCH-R530C
UCCT9V	SCH-R530C
UD8CCH	SCH-R530C
ULK4ZV	SCH-R530C
WLY9DQ	SCH-R530C [Databases\settings.db\system\device_name]
XPRVJJ	SCH-R530C
ZYQ8TH	SAMR530C

TABLE 1

Question 3 - Phone settings

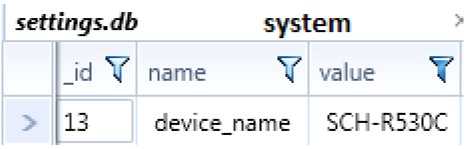
Consensus Result: SCH-R530C

Expected Response Explanation:

The device name can be found in the settings.db database under the system table. This file can be found at: root\data\com.android.providers.settings\databases\settings.db

Some participants identified the name of the device as either "Steve Lefft" or "SAMR530C". However, "Steve Lefft" is the name of the suspect (owner of the device) and SAMR530C refers to the brand Samsung and the model R530C. Niether one is the device name as reported by the phone.

Expected Response Illustration:



settings.db system

_id	name	value
13	device_name	SCH-R530C

TABLE 1

Question 4 - Phone settings

Question 4: What is the Bluetooth address for the phone?

Manufacturer's Expected Response: 94:01:C2:2F:94:FC

WebCode	Response
2HZNCM	94:01:C2:2F:94:FC
2MX9EK	94:01:c2:2f:94:fc
2W2HLB	94:01:C2:2F:94:FC
3JPC9M	94:01:C2:2F:94:FC
3UP3RA	94:01:C2:2F:94:FC
6GECZL	94:01:c2:2f:94:fc
6HAU49	94:01:C2:2F:94:FC
7TLJFH	94:01:C2:2F:94:FC
9MAA37	94:01:C2:2F:94:FC
ATTZ37	94:01:C2:2F:94:FC
BDWZNC	94:01:C2:2F:94:FC
EXQ8BW	94:01:C2:2F:94:FC
EZFET9	94:01:C2:2F:94:FC
FFMX46	94:01:c2:2f:94:fc
FHB8E7	94:01:C2:2F:94:FC
H46R9T	94:01:C2:2F:94:FC
H47R79	94:01:C2:2F:94:FC
JVM7CV	94:01:C2:2F:94:FC
LHAK2Z	94:01:C2:2F:94:FC
LJ7ZDX	94:01:C2:2F:94:FC
NQYVN2	94:01:C2:2F:94:FC
R6PT4T	94:01:C2:2F:94:FC
RECRVY	94:01:C2:2F:94:FC
RY2BNW	94:01:c2:2f:94:FC
RYWRZT	94:01:C2:2F:94:FC
TCHNEW	94:01:C2:2F:94:FC
UCCT9V	94:01:C2:2F:94:FC
UD8CCH	94:01:C2:2F:94:FC
ULK4ZV	94:01:c2:2f:94:fc
WLY9DQ	94:01:C2:2F:94:FC [Databases\settings.db\secure\bluethooth_address]
XPRVJJ	94:01:C2:2F:94:FC
ZYQ8TH	94:01:C2:2F:94:FC

TABLE 1

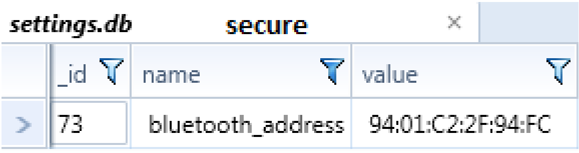
Question 4 - Phone settings

Consensus Result: 94:01:C2:2F:94:FC

Expected Response Explanation:

The Bluetooth address can be found in the settings.db database under the secure table. This file can be found at: root\data\com.android.providers.settings\databases\settings.db

Expected Response Illustration:



settings.db secure

_id	name	value
73	bluetooth_address	94:01:C2:2F:94:FC

TABLE 1

Question 5 - Phone settings

Question 5: What time zone is the phone configured for? (Provide the answer as GMT +/- hours)

<u>Manufacturer's Expected Response</u>: GMT -5

WebCode	Response
2HZNCM	-5
2MX9EK	GMT -5 :00
2W2HLB	GMT -5
3JPC9M	GMT -5
3UP3RA	GMT -5
6GECZL	GMT -5
6HAU49	GMT -5
7TLJFH	GMT -5 hours
9MAA37	GMT -5
ATTZ37	GMT -5:00
BDWZNC	GMT -5
EXQ8BW	GMT -5
EZFET9	GMT -5
FFMX46	GMT -5
FHB8E7	GMT -5 hours
H46R9T	America/New_York
H47R79	GMT -5
JVM7CV	AMERICA / NEW YORK GTM -4
LHAK2Z	GMT -5
LJ7ZDX	GMT -5 Hours (America/New York)
NQYVN2	GMT -5
R6PT4T	GMT -5
RECRVY	GMT -5 hours
RY2BNW	America/New_York GMT -5
RYWRZT	New York/America UTC+0
TCHNEW	GMT -5
UCCT9V	The timezone is set to America/New York which during the event of this case is set to GMT -5. Note that America/New York during the Summer Months is set to GMT-4 (Eastern Daylight Time).
UD8CCH	America/New_York (GMT -05 :00)
ULK4ZV	GMT -5
WLY9DQ	America/New York (Estern Standard Time) Activated 12/10/14 04:00:04 PM (UTC+0) = same time as GMT [Device Info\Time Zone]
XPRVJJ	GMT -5:00
ZYQ8TH	GMT -5

TABLE 1

Question 5 - Phone settings

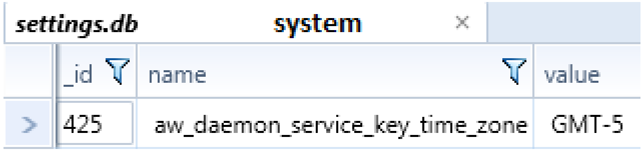
Consensus Result: GMT -5

Expected Response Explanation:

The question asks for the response to be presented in GMT +/- hours. The incident occurred in December of 2014; the season of Eastern Standard Time (EST). EST is five hours behind universal time, and is represented by GMT -5. However, analysis of the data was conducted during Eastern Daylight Time (EDT). EDT is four hours behind universal time and is represented by GMT -4. This could cause some variation in responses including GMT -5, GMT -4, and UTC time.

The time zone can be found in the settings.db database under the system table. This file can be found at: root\data\com.android.providers.settings\databases\settings.db

Expected Response Illustration:



_id	name	value
425	aw_daemon_service_key_time_zone	GMT-5

TABLE 1

Question 6 - Phone settings

Question 6: What city was the phone located in when it was last turned on? (As provided in the android providers' settings)

Manufacturer's Expected Response: Cascades

WebCode	Response
2HZNCM	Cascades
2MX9EK	Cascades, VA
2W2HLB	Cascades
3JPC9M	Cascades
3UP3RA	Cascades, New York
6GECZL	Sterling, VA
6HAU49	Cascades
7TLJFH	Cascades
9MAA37	Cascades, Virginia, USA
ATTZ37	Cascades, Virginia
BDWZNC	Cascades
EXQ8BW	CASCADES
EZFET9	Not Available
FFMX46	Cascades
FHB8E7	Cascades
H46R9T	Virginia (cityId:2274802)
H47R79	Cascades (Virginia, USA)
JVM7CV	POTOMAC FALLS, VA 20165 EEUU
LHAK2Z	Cascades
LJ7ZDX	Cascades
NQYVN2	Cascades
R6PT4T	Cascades, VA
RECRVY	Sterling, VA
RY2BNW	Cascades
RYWRZT	Sterling, Virginia
TCHNEW	Cascades
UCCT9V	Dulles Town Center. (Please see comments).
UD8CCH	Cascades
ULK4ZV	Cascades
WLY9DQ	New York (America)
XPRVJJ	Cascades, Virginia
ZYQ8TH	Cascades

TABLE 1

Question 6 - Phone settings

Consensus Result: No Consensus Reached

Expected Response Explanation:

No consensus was reached for question 6. Majority of the responses can be placed in groups based on similar patterns. Variation seen for this question is due to location examiner pulled the data from and how tool used reports the information. Below is a breakdown of the patterns seen in the responses given:

Response for this group can be found at: root\data\com.android.providers.settings\databases\settings.db – system table

- Cascades – 17 participants
- Cascades, VA – 6 participants
- Virginia (cityid: 2274808) – 1 participant

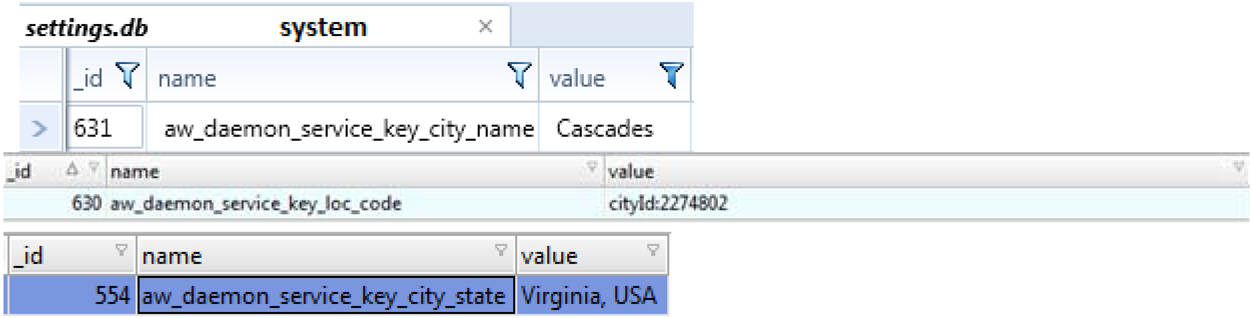
Responses for this group will reflect various tool reporting methods:

- Sterling, VA – 3 participants
- Potomac Falls, VA 20165 EEUU – 1 participant
- Dulles Town Center -1 participant
- Cascades, New York – 1 participant
- New York (America) – 1 participant
- Not Available – 1 participant

Information about the phone's current city can be found in the settings.db database. The system table holds a key with the name aw_daemon_service_key_city_name and the value of that key is the city where the phone was located when it was last turned on.
This file can be found at: root\data\com.android.providers.settings\databases\settings.db
The above mentioned path will show the State, City, and City ID.

Other areas in Virginia such as Sterling, Dulles Town Center, and Potomac Falls were areas of activity, but not the location the device reports as the last place it was turned on.

Expected Response Illustration:



_id	name	value
631	aw_daemon_service_key_city_name	Cascades

_id	name	value
630	aw_daemon_service_key_loc_code	cityId:2274802

_id	name	value
554	aw_daemon_service_key_city_state	Virginia, USA

TABLE 1

Question 7 - Phone settings

Question 7: What is the active Gmail account on the phone?

Manufacturer's Expected Response: lefty21331@gmail.com

WebCode	Response
2HZNCM	Lefty21331@gmail.com
2MX9EK	lefty21331@gmail.com
2W2HLB	lefty21331@gmail.com
3JPC9M	lefty21331@gmail.com
3UP3RA	lefty21331@gmail.com
6GECZL	lefty21331@gmail.com
6HAU49	lefty21331@gmail.com
7TLJFH	lefty21331@gmail.com
9MAA37	lefty21331@gmail.com
ATTZ37	"Steve Lefft" lefty21331@gmail.com
BDWZNC	lefty21331@gmail.com
EXQ8BW	lefty21331@gmail.com
EZFET9	lefty21331@gmail.com
FFMX46	lefty21331@gmail.com
FHB8E7	lefty21331@gmail.com
H46R9T	lefty21331@gmail.com
H47R79	lefty21331@gmail.com
JVM7CV	lefty21331@gmail.com
LHAK2Z	lefty21331@gmail.com
LJ7ZDX	lefty21331@gmail.com
NQYVN2	lefty21331@gmail.com
R6PT4T	lefty21331@gmail.com
RECRVY	lefty21331@gmail.com
RY2BNW	lefty21331@gmail.com
RYWRZT	lefty21331@gmail.com
TCHNEW	lefty21331@gmail.com
UCCT9V	lefty21331@gmail.com
UD8CCH	lefty21331@gmail.com
ULK4ZV	lefty21331@gmail.com
WLY9DQ	lefty21331@gmail.com [Emails] &[Text\settings_preference.xml]
XPRVJJ	"Steve Lefft" lefty21331@gmail.com
ZYQ8TH	lefty21331@gmail.com

TABLE 1

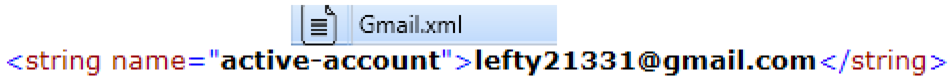
Question 7 - Phone settings

Consensus Result: lefty21331@gmail.com

Expected Response Explanation:

Information about the active Gmail account can be found in the Gmail.xml file. In this file there is a string name “active-account” with the value lefty21331@gmail.com
This file can be found at: root\data\com.google.android.gm\shared_prefs\Gmail.xml

Expected Response Illustration:



```
<string name="active-account">lefty21331@gmail.com</string>
```

TABLE 1

Question 8 - Phone settings

Question 8: What was the last application that the suspect Steven Lefft downloaded? (Provide the application's package name)

Manufacturer's Expected Response: com.konylabs.capitalone

WebCode	Response
2HZNCM	com.konylabs.capitalone-1.apk
2MX9EK	com.konylabs.capitalone-1.apk
2W2HLB	com.konylabs.capitalone-1.apk
3JPC9M	com.konylabs.capitalone-1.apk
3UP3RA	com.konylabs.capitalone-1.apk
6GECZL	Capital One® Mobile
6HAU49	com.konylabs.capitalone
7TLJFH	com.konylabs.capitalone
9MAA37	com.konylabs.capitalone-1.apk
ATTZ37	com.konylabs.capitalone "Capital One Mobile Banking App"
BDWZNC	com.konylabs.capitalone-1.apk
EXQ8BW	com.konylabs.capitalone-1.apk
EZFET9	com.konylabs.capitolone-1.apk
FFMX46	com.konylabs.capitalone-1.apk
FHB8E7	com.konylabs.capitalone (Capital One Mobile)
H46R9T	capitalone/.EnterpriseMobileBanking
H47R79	com.konylabs.capitalone-1.apk
JVM7CV	com.konylabs.capitalone
LHAK2Z	com.konylabs.capitalone-1.apk/Captial One Mobile
LJ7ZDX	com.konylabs.capitalone
NQYVN2	com.konylabs.capitalone
R6PT4T	Capital One Mobile
RECRVY	capitalone-1.apk
RY2BNW	Capital One® Mobile /com.konylabs.capitalone-1.apk
RYWRZT	Capital One Mobile (com.android.vending-com.konylabs.capitalone)
TCHNEW	com.konylabs.capitalone
UCCT9V	com.konylabs.capitalone-1.apk
UD8CCH	com.konylabs.capitalone-1.apk
ULK4ZV	com.konylabs.capitalone-1.apk
WLY9DQ	Capital One Mobile com.konylabs.capitalone [Installed Applications\ Captitol One Mobile v4.14.1…\Purchase date 12/11/2014…]
XPRVJJ	com.konylabs.capitalone "Capital One Mobile Banking App"
ZYQ8TH	com.konylabs.capitalone

TABLE 1

Question 8 - Phone settings

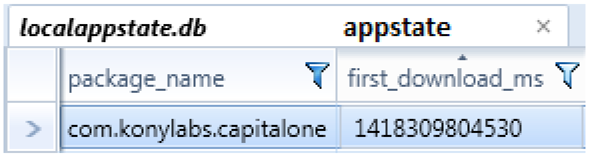
Consensus Result: com.konylabs.capitalone

Expected Response Explanation:

The expected response is looking for the name of the application package, and not just the application name. "Capital One Mobile" is the name of the application not the application package name.

Information on the last downloaded application, including the package name, can be seen in the localappstate.db in the appstate table. The localappstate.db database can be found at: root\data\com.android.vending\databases\localappstate.db

Expected Response Illustration:



localappstate.db appstate

package_name	first_download_ms
com.konylabs.capitalone	1418309804530

TABLE 1

Question 9 - Misc.

Question 9: Did the suspect Steven Lefft add the victim Harris Marvins as a contact in his phone book?

Manufacturer's Expected Response: Yes

WebCode	Response
2HZNCM	Yes
2MX9EK	Yes
2W2HLB	Yes
3JPC9M	Yes
3UP3RA	Yes
6GECZL	Yes
6HAU49	Yes
7TLJFH	Yes
9MAA37	Yes as "Harris" this is by name no reference number has been provided in the scenario.
ATTZ37	Yes
BDWZNC	Yes
EXQ8BW	Yes
EZFET9	Yes
FFMX46	Yes
FHB8E7	Yes
H46R9T	Yes, The phone no. is 5712129673
H47R79	Yes
JVM7CV	YES, Mobile: 5712129673
LHAK2Z	Yes
LJ7ZDX	Yes (5712129673)
NQYVN2	Yes
R6PT4T	Yes
RECRVY	Yes, phone 571-212-9673
RY2BNW	Yes
RYWRZT	Yes
TCHNEW	yes
UCCT9V	A person by the name of “Harris” with mobile phone number: '5712129673' was added to the phonebook. An MMS (text message) was sent to this phone number and addressed the recipient as Mr. Marvins. Without more information (such as Mr Harris Marvins phone number) it is not possible to ascertain if this is indeed Mr. Harris Marvins.
UD8CCH	Contact name Harris (Phone Number : 5712129673) is added in the contact list but not with complete name as Harris Marvins. However, this contact number can be confirmed to be Harris Marvins’s contact number from SMS conversation with PAUL.
ULK4ZV	Yes
WLY9DQ	Yes- A contact marked "Harris" with Mobile: 6712129673 was observed harris.marvins@aol.com was noted under emails
XPRVJJ	Yes

TABLE 1

Question 9 - Misc.

WebCode	Response
ZYQ8TH	There is an entry for Harris in contacts with a phone number of 5712129673

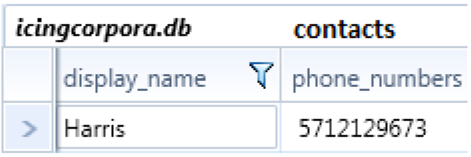
Consensus Result: Yes

Expected Response Explanation:

Information on Steve's phone contact list can be found in the icingcorpora.db database under the contacts table.

The icingcorpora.db database can be found at:
root\data\com.google.android.googlequicksearchbox\databases\icingcorpora.db

Expected Response Illustration:



icingcorpora.db	contacts
display_name	phone_numbers
Harris	5712129673

TABLE 1

Question 10 - Misc.

Question 10: The suspect Steven Lefft connected to a wireless network with the SSID “HideoutHotspot”. What was the password for this wireless network?

Manufacturer's Expected Response: 123steal

WebCode	Response
2HZNCM	123steal
2MX9EK	123steal
2W2HLB	123steal
3JPC9M	123steal
3UP3RA	123steal
6GECZL	13steal
6HAU49	123steal
7TLJFH	123steal
9MAA37	123steal
ATTZ37	123steal
BDWZNC	123steal
EXQ8BW	123steal
EZFET9	123steal
FFMX46	123steal
FHB8E7	123steal
H46R9T	123steal
H47R79	123steal
JVM7CV	123steal
LHAK2Z	123steal
LJ7ZDX	123steal
NQYVN2	123steal
R6PT4T	123steal
RECRVY	123steal
RY2BNW	123steal
RYWRZT	123steal
TCHNEW	123steal
UCCT9V	123steal
UD8CCH	123steal
ULK4ZV	123steal
WLY9DQ	123steal [Passwords\HideoutHotspot]
XPRVJJ	123steal
ZYQ8TH	123steal

TABLE 1

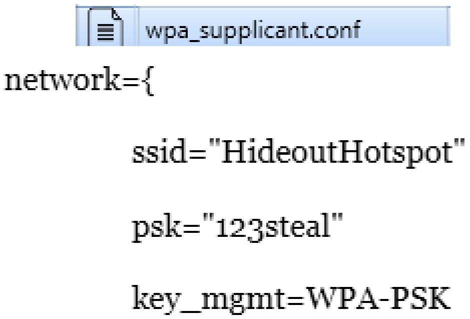
Question 10 - Misc.

Consensus Result: 123steal

Expected Response Explanation:

Information about what wireless networks Steve connected to can be found in the wpa_supplicant.conf file. The wpa_supplicant.conf file can be found at: root\misc\wifi\wpa_supplicant.conf

Expected Response Illustration:



wpa_supplicant.conf

```
network={
        ssid="HideoutHotspot"
        psk="123steal"
        key_mgmt=WPA-PSK
```

TABLE 1

Question 11 - Misc.

Question 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?

Manufacturer's Expected Response: dadami’s iPhone

WebCode	Response
2HZNCM	dadami’s iPhone
2MX9EK	dadami’s iPhone
2W2HLB	dadami's iPhone
3JPC9M	dadami's iPhone
3UP3RA	Dadami’s iphone
6GECZL	dadami’s iphone
6HAU49	dadami’s iPhone
7TLJFH	dadami's iPhone
9MAA37	dadami's iPhone
ATTZ37	dadami's iPhone
BDWZNC	dadami's iPhone
EXQ8BW	dadami's iPhone
EZFET9	dadami's iphone
FFMX46	dadami’s iPhone
FHB8E7	dadami's iPhone
H46R9T	SCH-R530C
H47R79	dadami’s IPhone
JVM7CV	dadami's iPhone
LHAK2Z	dadami's iPhone
LJ7ZDX	68:9C:70:D8:6B:08
NQYVN2	dadami’s iPhone
R6PT4T	AndroidAP
RECRVY	dadamiâ€™s iPhone 68:9c:70:d8:6b:08
RY2BNW	dadami’s iPhone I did not see any evidence showing it completed connecting or did not complete connection.
RYWRZT	
TCHNEW	dadami’s iPhone
UCCT9V	dadami’s iPhone
UD8CCH	dadami’s iPhone
ULK4ZV	dadami's iPhone
WLY9DQ	AndroidAp
XPRVJJ	dadimi's iPhone
ZYQ8TH	dadami’s iPhone

TABLE 1

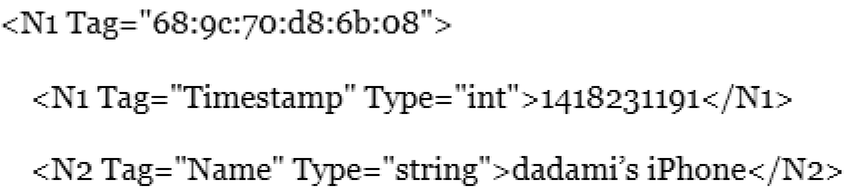
Question 11 - Misc.

Consensus Result: dadami’s iPhone

Expected Response Explanation:

Information about Bluetooth connections can be found in the bt_config.old file. This file can be found at: File:root\misc\bluedroid\bt_config.old
The expected response was for the Name of the phone, as represented in the images below by the N2 Tag="Name" field.

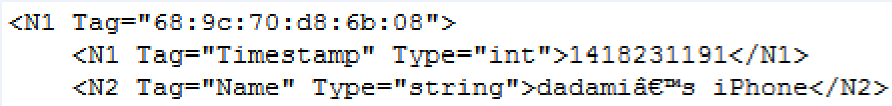
Expected Response Illustration:



```
<N1 Tag="68:9c:70:d8:6b:08">

   <N1 Tag="Timestamp" Type="int">1418231191</N1>

   <N2 Tag="Name" Type="string">dadami’s iPhone</N2>
```



```
<N1 Tag="68:9c:70:d8:6b:08">
    <N1 Tag="Timestamp" Type="int">1418231191</N1>
    <N2 Tag="Name" Type="string">dadamiâ€™s iPhone</N2>
```

TABLE 1

Question 12 - Misc.

Question 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)

Manufacturer's Expected Response: 11-12-2014 15:53:18

WebCode	Response
2HZNCM	12-12-2014 09:14:59
2MX9EK	10-12-2014 (10-Dec-2014), 15:39:12
2W2HLB	12-11-2014 15:53:18
3JPC9M	11-12-2014 8:24:52
3UP3RA	12-11-2014 15:53:18
6GECZL	11-12-2014 8:36:23 AM
6HAU49	11-12-2014 15:53:18
7TLJFH	11-12-2014 15:53:18
9MAA37	11-12-2014 15:53:18
ATTZ37	11-12-2014 08:24:52
BDWZNC	11-12-2014 15:53:18 GMT-0500
EXQ8BW	12-11-2014 15:53:18
EZFET9	12-11-2014 08:24:45
FFMX46	11-12-2014 08:24:46
FHB8E7	11/12/2014 15:53:18 (UTC-5)
H46R9T	11/12/2014 13:33
H47R79	11-12-2014 12:25:30
JVM7CV	11-12-2014 / 20:53:28(UTC+0) // 11-12-2014 / 16:53:28(local time)
LHAK2Z	11-12-2014 (11-Dec-2014)/15:53:18
LJ7ZDX	11-12-2014 at 12:25:30 h.
NQYVN2	11-12-2014 15:53:18 -0500
R6PT4T	11-12-2014 15:53:18
RECRVY	12/11/2014 8:24:45
RY2BNW	12-12-2014 9:14:59
RYWRZT	12-11-2014 08:53:18
TCHNEW	11 /12/ 2014 15:53:19 -0500 (Dec 11, 2014)
UCCT9V	Viber was last started on 11-12-2014 08:24:45 (GMT-5), however according to Viber the app was running at 11-12-2014 08:24:52 (GMT-5). Please see comments.
UD8CCH	11-12-2014 15:53:18 (GMT - 05:00)
ULK4ZV	11-12-2014 08:24:52
WLY9DQ	11/12/2014 12:25:30 (UTC --5) -> adjusted to eastern time [Timeline\ Instant Messages]
XPRVJJ	11-12-2014 08:24:52
ZYQ8TH	12/11/2014 15:53:18 (UTC-5)

TABLE 1

Question 12 - Misc.

Consensus Result: No Consensus Reached

Expected Response Explanation:

No consensus was reached for question 12. Majority of the responses can be placed in groups based on similar patterns. Variation seen for this question is due to examiner interpretation of the question being asked, and the format of the given response. Below is a breakdown of the patterns seen in the responses given:

Unconverted response for this group can be found at: root\system\dmappmgr.db – ApplicationControl table- Last Launch Time

- 11-12-2014 15:53:18 – 9 participants
- 11-12-2014 15:53:19 – 1 participant
- 11-12-2014 20:53:28 (UTC +0) / 16:53:28 (local time) – 1 participant
- 12-11-2014 15:53:18 – 4 participants

Unconverted response for this group can be found at: root\data\com.viber.voip\databases\viber_messages –adx table – Launch – Last Tracked

- 11-12-2014 8:24:52 – 5 participants (1 participant from this group included two answers)

Unconverted response for this group can be found at: root\system\dmappmgr.db – ApplicationControl table- App Last Service Start Time

- 12-11-2014 08:24:45 -2 participants
- 11-12-2014 08:24:45 -1 participant (participant contained two answers)
- 11-12-2014 08:24:46 – 1 participant

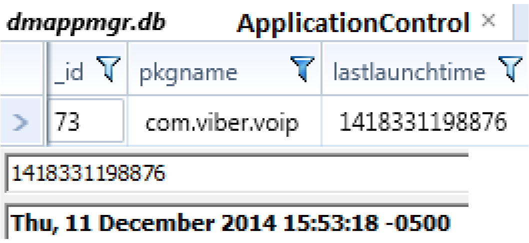
Unconverted response for this group can be found at: root\data\com.viber.voip\databases\viber_messages –conversations-date

- 11-12-2014 12:50:30 – 3 participants

The remaining six participants did not have recurring patterns and were not included in this breakdown.

The expected response is looking to present the last time the application was launched, not necessarily the last time the application was used. The question also asks for the response to be presented in dd-mm-yyyy format, as this is the universal format, as opposed to the mm-dd-yyyy format. Information about when the Viber app was last launched can be found in the dmappmgr.db database. The ApplicationControl table contains information about all of the apps on the phone. In the table there is a field detailing the last launch time for each application. This field contains a timestamp stored in a Unix Epoch time format which must be converted into the requested time and date format. This file can be found at: root\system\dmappmgr.db

Expected Response Illustration:



_id	pkgname	lastlaunchtime
73	com.viber.voip	1418331198876

1418331198876

Thu, 11 December 2014 15:53:18 -0500

TABLE 1

Question 13 - Misc.

Question 13: The suspect Steven Lefft copied a phone number to his clipboard, what was the phone number? (Provide the number as it is displayed)

Manufacturer's Expected Response: 5712129673

WebCode	Response
2HZNCM	5712129673
2MX9EK	5712129673
2W2HLB	5712129673
3JPC9M	571-212-9673
3UP3RA	5712129673
6GECZL	5712129673
6HAU49	5712129673
7TLJFH	5712129673
9MAA37	5712129673
ATTZ37	5712129673
BDWZNC	5712129673
EXQ8BW	5712129673
EZFET9	5712129673
FFMX46	5712129673
FHB8E7	5712129673
H46R9T	The phone no. is 17038551105.
H47R79	5712129673
JVM7CV	5712129673
LHAK2Z	5712129673
LJ7ZDX	5712129673
NQYVN2	5712129673
R6PT4T	5712129673
RECRVY	
RY2BNW	5712129673
RYWRZT	
TCHNEW	5712129673
UCCT9V	5712129673
UD8CCH	5712129673
ULK4ZV	5712129673
WLY9DQ	The number appears to be "5712129673" under Hew view [file system\ Image\ Root\ clipboard\ 1136702528217_598_179\clip]
XPRVJJ	5712129673
ZYQ8TH	5712129673

TABLE 1

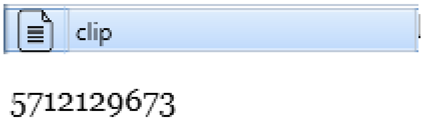
Question 13 - Misc.

Consensus Result: 5712129673

Expected Response Explanation:

Information about data that was copied to the clipboard can be found under the clipboard folder. The clipboard entry 113670252817_598_179 contains a phone number.
This file can be found at: root\clipboard\113670252817_598_179\clip

Expected Response Illustration:



5712129673

TABLE 1

Question 14 - Misc.

Question 14: What terms did the suspect Steven Lefft search in the Google Play store?

Manufacturer's Expected Response: email, viber, banks

WebCode	Response
2HZNCM	banks, viber, email
2MX9EK	banks, viber, email
2W2HLB	banks, viber, email
3JPC9M	
3UP3RA	Banks, viber, and email
6GECZL	Banks, viber, email
6HAU49	email, viber, banks
7TLJFH	banks, viber, email
9MAA37	banks, viber and email
ATTZ37	email, viber, banks
BDWZNC	banks, viber, email
EXQ8BW	banks, viber, email
EZFET9	banks, viber, email
FFMX46	email,viber,banks
FHB8E7	banks, email, viber
H46R9T	capital one mobile banking
H47R79	banks, viber, email
JVM7CV	banks / viber / email
LHAK2Z	banks, email, viber
LJ7ZDX	banks; viber; email
NQYVN2	email, viber, and banks
R6PT4T	banks viber email
RECRVY	1. banks, viber, email
RY2BNW	banks, viber, email
RYWRZT	banks, viber, email
TCHNEW	banks, email, viber
UCCT9V	Banks, viber, email
UD8CCH	banks, email, viber
ULK4ZV	email, viber, banks
WLY9DQ	"banks" "viber" "email" searched on Play Market [Searched Items\ Play Market]
XPRVJJ	email, viber, banks
ZYQ8TH	banks, viber, email

TABLE 1

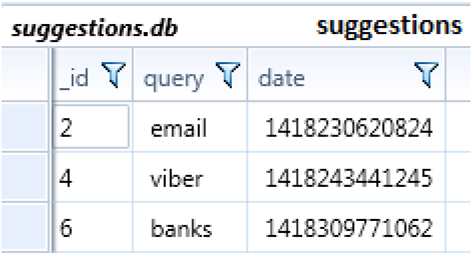
Question 14 - Misc.

Consensus Result: email, viber, banks

Expected Response Explanation:

Information about what was searched in the Google Play store can be found in the suggestions.db database. The suggestions table contains all of the keywords that were searched.
This file can be found at: root\data\com.android.vending\databases\suggestions.db

Expected Response Illustration:



suggestions.db suggestions

_id	query	date
2	email	1418230620824
4	viber	1418243441245
6	banks	1418309771062

TABLE 1

Question 15 - Misc.

Question 15: Provide the coordinates where the picture “20141211_141619.jpg” was taken? (Format exactly as displayed in the EXIF data)

Manufacturer's Expected Response: Latitude 39" 1' 31.952
Longitude 77" 24' 7.328

WebCode	Response
2HZNCM	Latitude 39; 1; 31.952 Longitude 77; 24; 7.328 Altitude 67.8
2MX9EK	(39.025542, -77.402036)
2W2HLB	(39.025542, -77.402036)
3JPC9M	39 1'31.952" 77 24'7.328"
3UP3RA	39.025542, -77.402036
6GECZL	(39.025542, -77.402036)
6HAU49	GpsLatitude: 39.000000 1.000000 31.952000 GpsLongitude: 77.000000 24.000000 7.328000
7TLJFH	39.025542 / -77.402036
9MAA37	As per UFED Lat/Lon (39.025542, -77.402036) from the EXIF data in more detail - Latitude N 39° 1' 0.9" Longitude W 77° 24' 0.7" = in hex from the EXIF: 27 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 D0 7C 00 00 E8 03 00 00 Hex latitude in EXIF = Degrees 39 Min 1 Seconds 32 | 4D 00 00 00 01 00 00 00 18 00 00 00 01 00 00 00 A0 1C 00 00 E8 03 00 00 Hex Longitude in EXIF = Degrees 77 Min 24 Sec 7 = (Lat 39.025542, Long -77.402036)
ATTZ37	Lat 39.0255N Long -77.4020W
BDWZNC	Latitude:39,1,31.952, Longitude:77,24,7.328
EXQ8BW	(39.025542, -77.402036)
EZFET9	39.025542, -77.402442
FFMX46	Latitude 39.02554222222222, Longitude -77.40203555555556, Altitude 67.8
FHB8E7	latitude: 39,1,31.952 longitude: 77,24,7.328
H46R9T	Latitude: N 39.025542; Longitude: W 77.402035
H47R79	GPS Latitude: 39,1,31.952 N; GPS Longitude: 77,24,7.328 W; GPS Altitude: 67,8
JVM7CV	39,1,31,952 N / 77,24,7,328 W
LHAK2Z	GPSLatitude 39,1,31.952/GPSLongitude 77,24,7.328
LJ7ZDX	32.025542, -77.402036
NQYVN2	Latitude: 39° 1' 31.952" N or 39.025542; Longitude: 77° 24' 7.328" W or -77.402036
R6PT4T	39.025542, -77.402036
RECRVY	(39.025542, -77.402036)
RY2BNW	GPSVersionID 2,2,0,0 GPSLatitude N, GPSLatitude 39,1,31.952, GPSLongitudeRef W, GPSLongitude 77,24,7.328, GPSAltitudeRef o, GPSAltitude 67.8, GPSTimeStamp 19,15,40, GPSProcessingMethod, ASCII, GPSDateStamp 2014:12:11
RYWRZT	(39.025542, -77.402036)
TCHNEW	N 39,1,31.952 W 77,24,7.328 GPSLatitudeRef - NGPSLatitude - 39 1 31.95 (39.025542)GPSLongitudeRef - WGPSLongitude -77 24 7.33 (77.402036)
UCCT9V	39° 1' 31.952" N, 77° 24' 7.328" W. Please see comments.
UD8CCH	N 39/1 1/1 31952/1000 , W 77/1 24/1 7328/1000 – According to FTK 4.0.2.33; Lat/Lon: (39.025542, -77.402036) – According to UFED Physical Analyzer 4.2.1.7
ULK4ZV	39.025542, -77.402036

TABLE 1

Question 15 - Misc.

WebCode	Response
WLY9DQ	GPSLatitudeRef N GPSLatitude 39, 1, 31.952 GPSLongitudeRef W GPSLongitude 77, 24, 7.328 GPSAltitudeRef 0 GPSAltitude 67, 8 GPSTimeStamp 19, 15, 40, GPSProcessingMethod ASCII GPSDateStamp 2014:12:11 Lat/Lon= (39.025542, -77.402036) [DCIM\Camera\20141211_141619.jpg]
XPRVJJ	Lat 39.0255N Long -77.4020W
ZYQ8TH	(39.025542, -77.402036)

Consensus Result: No Consensus Reached

Expected Response Explanation:

No consensus was reached for question 15. Majority of the responses can be placed in groups based on similar patterns. Variation seen for this question is due to coordinate conversions, location of where the coordinates were found, and tool used. Below is a breakdown of the patterns seen in the responses given:

Unconverted response for this group can be found at:
root\media\0\DCIM\Camera\20141211_141619.jpg

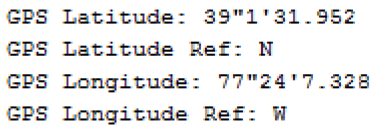
- Latitude 39; 1; 31.952 and Longitude 77; 24; 7.328 – 12 participants (3 participants also presented data in the format from next group)
- N 39/1 1/1 31952/1000 and W 77/1 24/1 7328/1000 – 1 participant (also presented data in format from next group)
- Latitude: 39.000000 1.000000 31.952000 and Longitude: 77.000000 24.000000 7.328000 – 1 participant

This groups presents the response as reported by the tool used and keeps the format:

- (39.025542, -77.402036) – 16 participants
- Latitude: N 39.025542; Longitude: W 77.402035 – 1 participant
- Lat 39.0255 N Long -77.4020W – 2 participants

The expected response was to be presented as reported by the EXIF data and not as presented by the tool. The coordinates of the picture can be located in the associated EXIF data. This file can be found at:
root\media\0\DCIM\Camera\20141211_141619.jpg

Expected Response Illustration:



```
GPS Latitude: 39"1'31.952
GPS Latitude Ref: N
GPS Longitude: 77"24'7.328
GPS Longitude Ref: W
```

TABLE 1

Question 16 - Misc.

Question 16: In Facebook Messenger, the suspect Steven Lefft sent Paul one message. Provide the coordinates associated with this message.

Manufacturer's Expected Response: latitude:39.030476
longitude:-77.40115

WebCode	Response
2HZNCM	(39.030476, -77.401150)
2MX9EK	(39.030476, -77.401150)
2W2HLB	(39.030476, -77.401150)
3JPC9M	39.0304762 -77.4011496
3UP3RA	39.030476, -77.401150
6GECZL	(39.030476, -77.401150)
6HAU49	Latitude: 39.030476 Longitude: -77.40115
7TLJFH	39.0304762 / -77.4011496
9MAA37	Latitude 39.030476, Longitude -77.401150
ATTZ37	latitude 39.030476 longitude -77.40115
BDWZNC	latitude:39.030476, longitude:-77.40115
EXQ8BW	(39.030476, -77.401150)
EZFET9	39.030476, -77.401150
FFMX46	{"latitude":39.0304762,"longitude":-77.4011496,"accuracy":1505.0}
FHB8E7	latitude: 39.0304762, longitude: -77.4011496, accuracy: 1505.0
H46R9T	Latitude: 39.02525; Longitude:-77.40218
H47R79	"latitude":39.0304762,"longitude":-77.4011496,"accuracy":1505.0
JVM7CV	39,030476 N / 77,40115 W
LHAK2Z	Latitude 39.0304762/Longitude -77.4011496 (accuracy: 1505.0)
LJ7ZDX	39.030476, -77.401150
NQYVN2	"latitude":39.0304762,"longitude":-77.4011496
R6PT4T	39.030476, -77.401150
RECRVY	(39.030476, -77.401150)
RY2BNW	39.030476, -77.401150
RYWRZT	(39.030476, -77.401150)
TCHNEW	"latitude":39.0304762,"longitude":-77.4011496,"accuracy":1505.0
UCCT9V	"latitude":39.0304762,"longitude":-77.4011496,"accuracy":1505.0
UD8CCH	Position: (39.030476, -77.401150) – According to UFED Physical Analyzer 4.2.1.7
ULK4ZV	39.030476, -77.40115
WLY9DQ	Coordinates= (39.030476, -77.401150) [Chats\ Facebook Messenger]
XPRVJJ	latitude 39.030476 longitude -77.40115
ZYQ8TH	(39.030476, -77.401150)

TABLE 1

Question 16 - Misc.

Consensus Result: No Consensus Reached

Expected Response Explanation:

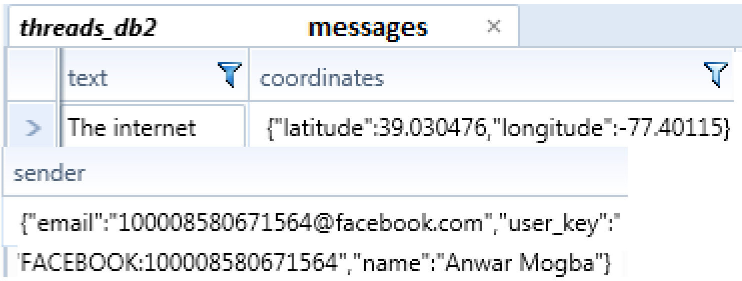
No consensus was reached for question 16. Majority of the responses can be placed into one group with varying conversion differences. Variation seen for this question is due to conversions , data source, and tool used. Below is a breakdown of the patterns seen in the responses given:

Unconverted response for this group can be found at: root\data\com.facebook.orca\databases\threads_db2 – messages table

- Latitude 39.030476, Longitude -77.401150 – 16 participants
- Latitude 39.030476, Longitude -77.40115 – 6 participants
- Latitude 39.0304762, Longitude -77.4011496 – 8 participants
- Latitude 39.02525, Longitude -77.40218 – 1 participant

Information about messages in Facebook Messenger can be seen in the threads_db2 database file under the messages table. In the messages table there is a field named coordinates. This field contains the GPS coordinates for the location of the device when the Facebook message was sent.
This file can be found at: root\data\com.facebook.orca\databases\threads_db2

Expected Response Illustration:



text	coordinates
The internet	{"latitude":39.030476,"longitude":-77.40115}

sender
{"email":"100008580671564@facebook.com","user_key":" FACEBOOK:100008580671564","name":"Anwar Mogba"}

TABLE 1

Question 17 - Applications

Question 17: The suspect Steven Lefft created a fake Facebook profile. What was the name of the Facebook profile?

Manufacturer's Expected Response: Anwar Mogba

WebCode	Response
2HZNCM	Anwar Mogba
2MX9EK	Anwar Mogba
2W2HLB	Anwar Mogba
3JPC9M	Anwar Mogba
3UP3RA	Anwar Mogba
6GECZL	Amwar Mogba
6HAU49	Anwar Mogba
7TLJFH	Anwar Mogba
9MAA37	Anwar Mogba
ATTZ37	Anwar Mogba
BDWZNC	Anwar Mogba
EXQ8BW	Anwar Mogba
EZFET9	Anwar Mogba
FFMX46	Anwar Mogba
FHB8E7	Anwar Mogba (www.facebook.com/anwar.mogba)
H46R9T	Full name: Anwar Mogba
H47R79	Anwar Mogba
JVM7CV	Anwar Mogba
LHAK2Z	www.facebook.com/anwar.mogba, Anwar Mogba
LJ7ZDX	Anwar Mogba
NQYVN2	Anwar Mogba
R6PT4T	Anwar Mogba
RECRVY	Anwar Mogba
RY2BNW	leftout21331@yahoo.com / Anwar Mogba
RYWRZT	Anwar Mogba
TCHNEW	Anwar Mogba
UCCT9V	Anwar Mogba
UD8CCH	Anwar Mogba
ULK4ZV	Anwar Mogba
WLY9DQ	Name= Anwar Mogba [User Accounts\Facebook]
XPRVJJ	Anwar Mogba
ZYQ8TH	Anwar Mogba

TABLE 1

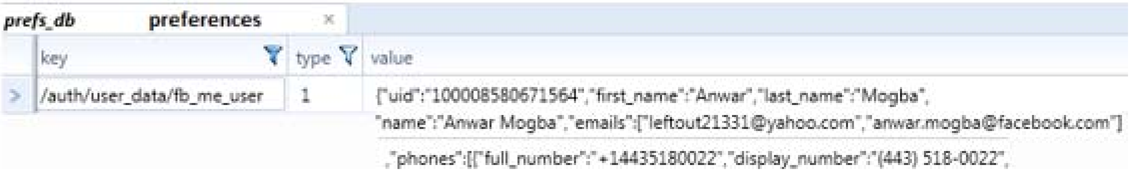
Question 17 - Applications

Consensus Result: Anwar Mogba

Expected Response Explanation:

The prefs_db database contains information about the Facebook app. The preferences table contains a key auth/user_data/fb_me_user the value for this key contains the name associated with the Facebook profile. This file can be found at: root\data\com.facebook.katana\databases\prefs_db

Expected Response Illustration:



prefs_db preferences

key	type	value
/auth/user_data/fb_me_user	1	{"uid":"100008580671564","first_name":"Anwar","last_name":"Mogba", "name":"Anwar Mogba","emails":["leftout21331@yahoo.com","anwar.mogba@facebook.com"] ,"phones":[{"full_number":"+14435180022","display_number":"(443) 518-0022",

TABLE 1

Question 18 - Applications

Question 18: What display phone number did the suspect Steven Lefft use to register with the Facebook application? (###) ###-####

<u>Manufacturer's Expected Response</u>: (443)518-0022

WebCode	Response
2HZNCM	(443)518-0022
2MX9EK	(443)518-0022
2W2HLB	(443)518-0022
3JPC9M	(443)518-0022
3UP3RA	(443)518-0022
6GECZL	(443)518-0022
6HAU49	(443)518-0022
7TLJFH	(443)518-0022
9MAA37	(443)518-0022
ATTZ37	(413)518-0022
BDWZNC	(443)518-0022
EXQ8BW	(443)518-0022
EZFET9	(443)518-0022
FFMX46	(443)518-0022
FHB8E7	(443)518-0022
H46R9T	14435180022
H47R79	(443)518-0022
JVM7CV	(443)518-0022
LHAK2Z	(443)518-0022
LJ7ZDX	(703) 855-1105
NQYVN2	443-518-0022
R6PT4T	(443)518-0022
RECRVY	(703) 855-1105
RY2BNW	(443)518-0022
RYWRZT	(443)518-0022
TCHNEW	Display number (443)518-0022
UCCT9V	(443)518-0022
UD8CCH	(443)518-0022
ULK4ZV	(443)518-0022
WLY9DQ	(443)518-0022 [Databases\#147\prefs_db\
XPRVJJ	(413)518-0022
ZYQ8TH	(443)518-0022

TABLE 1

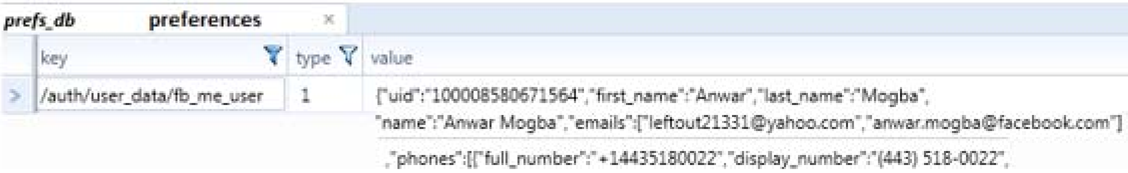
Question 18 - Applications

Consensus Result: (443)518-0022

Expected Response Explanation:

In the prefs_db database under the preferences table there is a key auth/user_data/fb_me_user. This key provides information about the current Facebook user, including their phone number (443)518-0022. The prefs_db file can be found at: root\data\com.facebook.katana\databases\prefs_db

Expected Response Illustration:



	key	type	value
>	/auth/user_data/fb_me_user	1	{"uid":"100008580671564","first_name":"Anwar","last_name":"Mogba", "name":"Anwar Mogba","emails":["leftout21331@yahoo.com","anwar.mogba@facebook.com"] ,"phones":[{"full_number":"+14435180022","display_number":"(443) 518-0022",

TABLE 1

Question 19 - Applications

Question 19: What email address did the suspect Steven Lefft use to register on Facebook?

Manufacturer's Expected Response: leftout21331@yahoo.com

WebCode	Response
2HZNCM	leftout21331@yahoo.com
2MX9EK	leftout21331@yahoo.com
2W2HLB	leftout21331@yahoo.com
3JPC9M	leftout21331@yahoo.com
3UP3RA	leftout21331@yahoo.com
6GECZL	leftout21331@yahoo.com
6HAU49	leftout21331@yahoo.com
7TLJFH	leftout21331@yahoo.com
9MAA37	leftout21331@yahoo.com
ATTZ37	leftout21331@yahoo.com
BDWZNC	leftout21331@yahoo.com
EXQ8BW	leftout21331@yahoo.com
EZFET9	leftout21331@yahoo.com
FFMX46	leftout21331@yahoo.com
FHB8E7	leftout21331@yahoo.com
H46R9T	leftout21331@yahoo.com
H47R79	leftout21331@yahoo.com
JVM7CV	leftout21331@yahoo.com
LHAK2Z	leftout21331@yahoo.com
LJ7ZDX	leftout21331@yahoo.com
NQYVN2	leftout21331@yahoo.com
R6PT4T	leftout21331@yahoo.com
RECRVY	leftout21331@yahoo.com
RY2BNW	leftout21331@yahoo.com
RYWRZT	leftout21331@yahoo.com
TCHNEW	Leftout21331@yahoo.com
UCCT9V	leftout21331@yahoo.com
UD8CCH	leftout21331@yahoo.com
ULK4ZV	leftout21331@yahoo.com
WLY9DQ	leftout21331@yahoo.com [Databases\#147\prefs_db]
XPRVJJ	leftout21331@yahoo.com
ZYQ8TH	leftout21331@yahoo.com

TABLE 1

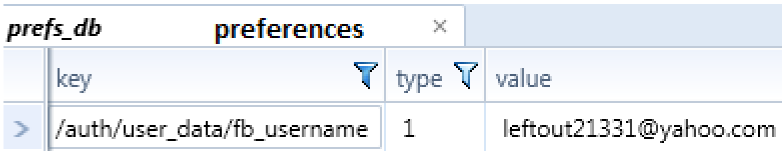
Question 19 - Applications

Consensus Result: leftout21331@yahoo.com

Expected Response Explanation:

Information regarding Steve's Facebook account can be found in the prefs_db database under the preferences table. In the preferences table there is a key "auth/user_data/fb_username" with the value leftout21331@yahoo.com. This is the email address that Steve used to register on Facebook. This file can be found at: root\data\com.facebook.katana\databases\prefs_db

Expected Response Illustration:



key	type	value
/auth/user_data/fb_username	1	leftout21331@yahoo.com

TABLE 1

Question 20 - Applications

Question 20: What is the suspect Steven Lefft's one Facebook friend's display name?

Manufacturer's Expected Response: Paul Gee

WebCode	Response
2HZNCM	Paul Gee
2MX9EK	Paul Gee
2W2HLB	Paul Gee
3JPC9M	Paul Gee
3UP3RA	Paul Gee
6GECZL	Paul Gee
6HAU49	Paul Gee
7TLJFH	Paul Gee
9MAA37	Paul Gee
ATTZ37	Paul Gee
BDWZNC	Paul Gee
EXQ8BW	Paul Gee
EZFET9	Paul Gee
FFMX46	Paul Gee
FHB8E7	Paul Gee
H46R9T	Full name: Paul Gee
H47R79	Paul Gee
JVM7CV	Paul Gee
LHAK2Z	Paul Gee
LJ7ZDX	Paul Gee
NQYVN2	Paul Gee
R6PT4T	Paul Gee
RECRVY	Paul Gee
RY2BNW	Paul Gee
RYWRZT	Paul Gee
TCHNEW	Paul Gee
UCCT9V	Paul Gee
UD8CCH	Paul Gee
ULK4ZV	Paul Gee
WLY9DQ	Paul Gee [Databases\contacts_db2]
XPRVJJ	Paul Gee
ZYQ8TH	Paul Gee

TABLE 1

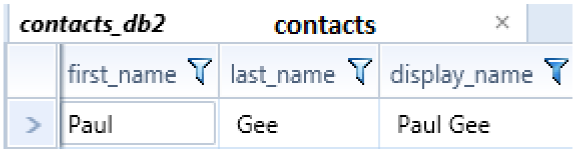
Question 20 - Applications

Consensus Result: Paul Gee

Expected Response Explanation:

Information about Steve's Facebook friends can be found in the contacts_db2 database under the contacts table. The contacts_db2 database can be found at:
root\data\com.facebook.katana\databases\contacts_db2

Expected Response Illustration:



first_name	last_name	display_name
Paul	Gee	Paul Gee

TABLE 1

Question 21 - Applications

Question 21: What did the suspect Steven Lefft search using Google? (Duplicate searches only need to be reported once)

Manufacturer's Expected Response: fraud, vacation homes

WebCode	Response
2HZNCM	Vacation homes, fraud
2MX9EK	vacation homes, fraud
2W2HLB	fraud, vacation homes
3JPC9M	fraud vacation homes
3UP3RA	Fraud and Vacation Homes
6GECZL	Fraud, vacation homes
6HAU49	vacation homes, fraud
7TLJFH	fraud, vacation homes
9MAA37	vacation homes and fraud
ATTZ37	fraud, vacation homes
BDWZNC	Vacation, homes, fraud
EXQ8BW	Fraud, vacation homes
EZFET9	Vacation Homes, Fraud
FFMX46	fraud,vacation homes
FHB8E7	vacation homes, fraud
H46R9T	fraud and vacation homes
H47R79	vacation homes, fraud
JVM7CV	fraud / vacation homes
LHAK2Z	Fraud, Vacation Homes
LJ7ZDX	vacation homes; fraud
NQYVN2	fraud, vacation homes
R6PT4T	fraud vacation homes
RECRVY	1.vacation homes 2. fraud
RY2BNW	fraud, vacation homes
RYWRZT	vacation homes, fraud
TCHNEW	vacation homes, fraud
UCCT9V	Vacation homes, fraud. Please see comments.
UD8CCH	fraud, vacation homes
ULK4ZV	
WLY9DQ	"fraud" "vacations home" [Searched Items\ Google Chrome]
XPRVJJ	fraud, vacation homes
ZYQ8TH	vacation homes, fraud

TABLE 1

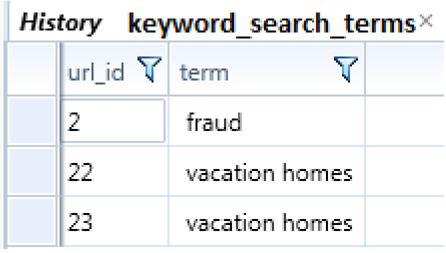
Question 21 - Applications

Consensus Result: fraud, vacation homes

Expected Response Explanation:

Information about search terms in Chrome can be found in the History database file under the keyword_search_terms table.
This file can be found at: root\data\com.android.chrome\app_chrome\Default\History

Expected Response Illustration:



History keyword_search_terms

url_id	term
2	fraud
22	vacation homes
23	vacation homes

TABLE 1

Question 22 - Applications

Question 22: In Chrome, what is the url of the first web page that the suspect Steven Lefft visited?

Manufacturer's Expected Response: http://www.justice.gov/criminal/fraud/websites/idtheft.html

WebCode	Response
2HZNCM	http://www.justice.gov/criminal/fraud/websites/idtheft.html
2MX9EK	http://www.justice.gov/criminal/fraud/websites/idtheft.html
2W2HLB	http://www.justice.gov/criminal/fraud/websites/idtheft.html
3JPC9M	http://www.justice.gov/criminal/fraud/websites/idtheft.html
3UP3RA	http://www.justice.gov/criminal/fraud/websites/idtheft.html
6GECZL	http://www.justice.gov/criminal/fraud/websites/idtheft.html
6HAU49	http://www.justice.gov/criminal/fraud/websites/idtheft.html
7TLJFH	http://www.justice.gov/criminal/fraud/websites/idtheft.html
9MAA37	http://www.justice.gov/criminal/fraud/websites/idtheft.html
ATTZ37	http://www.justice.gov/criminal/fraud/websites/idtheft.html
BDWZNC	http://www.justice.gov/criminal/fraud/websites/idtheft.html
EXQ8BW	http://www.justice.gov/criminal/fraud/websites/idtheft.html
EZFET9	http://www.justice.gov/criminal/fraud/websites/idtheft.html
FFMX46	http://www.justice.gov/criminal/fraud/websites/idtheft.html
FHB8E7	http://www.justice.gov/criminal/fraud/websites/idtheft.html
H46R9T	http://www.justice.gov/criminal/fraud/websites/idtheft.html
H47R79	http://www.justice.gov/criminal/fraud/websites/idtheft.html
JVM7CV	http://www.justice.gov/criminal/fraud/websites/idtheft.html
LHAK2Z	http://www.justice.gov/criminal/fraud/websites/idtheft.html
LJ7ZDX	http://www.justice.gov/criminal/fraud/websites/idtheft.html
NQYVN2	http://www.justice.gov/criminal/fraud/websites/idtheft.html
R6PT4T	http://www.justice.gov/criminal/fraud/websites/idtheft.html
RECRVY	http://www.justice.gov/criminal/fraud/websites/idtheft.html
RY2BNW	http://www.justice.gov/criminal/fraud/websites/idtheft.html
RYWRZT	https://banking.capitalone.com/
TCHNEW	http://www.justice.gov/criminal/fraud/websites/idtheft.html
UCCT9V	http://www.justice.gov/criminal/fraud/websites/idtheft.html
UD8CCH	http://www.justice.gov/criminal/fraud/websites/idtheft.html
ULK4ZV	
WLY9DQ	http://www.justice.gov/criminal/fraud/websites/idtheft.html (Last visited 12/11/2014 7:24:42 AM(UTC-8) [Databases\#83\History\]
XPRVJJ	http://www.justice.gov/criminal/fraud/websites/idtheft.html
ZYQ8TH	www.justice.gov/criminal/fraud/websites/idtheft.html

TABLE 1

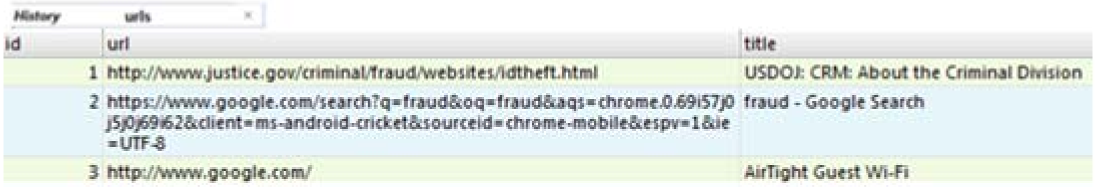
Question 22 - Applications

Consensus Result: http://www.justice.gov/criminal/fraud/websites/idtheft.html

Expected Response Explanation:

Information on the first web page visited in Chrome can be found in the History database file under the urls table. This file can be found at: root\data\com.android.chrome\app_chrome\Default\History

Expected Response Illustration:



id	url	title
1	http://www.justice.gov/criminal/fraud/websites/idtheft.html	USDOJ: CRM: About the Criminal Division
2	https://www.google.com/search?q=fraud&oq=fraud&aqs=chrome.0.69i57j0j5j0j69i62&client=ms-android-cricket&sourceid=chrome-mobile&espv=1&ie=UTF-8	fraud - Google Search
3	http://www.google.com/	AirTight Guest Wi-Fi

TABLE 1

Question 23 - Applications

Question 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)

Manufacturer's Expected Response: 11-12-2014 10:24:42

WebCode	Response
2HZNCM	11-12-2014 10:24:42 hrs
2MX9EK	11-12-2014 (11 Dec 2014) 10:24:42
2W2HLB	12-11-2014 10:24:42
3JPC9M	12-11-2014 15:24:42
3UP3RA	12-11-2014 10:24:42
6GECZL	11-12-2014 10:24:42 AM
6HAU49	11-12-2014 10:24:42
7TLJFH	11-12-2014 10:24:42
9MAA37	11-12-2014 10:24:42
ATTZ37	11-12-2014 10:24:42
BDWZNC	11-12-2014 10:24:42 GMT-0500
EXQ8BW	12-11-2014 10:24:42
EZFET9	12-11-2014 10:24:42
FFMX46	11-12-2014 10:24:42
FHB8E7	11/12/2014 10:24:42 (UTC-5)
H46R9T	11/12/2014 15:24
H47R79	11-12-2014 10:24:42
JVM7CV	11-12-2014 / 15:24:42 (UTC+0) // 11-12-2014 / 11:24:42 (local time)
LHAK2Z	11-12-2014 (11-Dec-2014)/10:24:42
LJ7ZDX	11-12-2014 at 10:24:42 hours
NQYVN2	11-12-2014 10:24:42 -0500
R6PT4T	11-12-2014 10:24:42
RECRVY	12/11/2014 10:24:42
RY2BNW	http://www.justice.gov/criminal/fraud/websites/idtheft.html11-12-2014 10:24:42 hours
RYWRZT	12/11/2014 03:24:42
TCHNEW	11/12/2014 10:24:42 AM(UTC -5) (Dec 11, 2014)
UCCT9V	11-12-2014 10:24:42(GMT-5)
UD8CCH	11-12-2014 10:24:42 (GMT - 05:00)
ULK4ZV	
WLY9DQ	US DOJ visited 11/12/2014 10:24:42 AM (UTS-5) [Web History\Google Chrome]
XPRVJJ	11-12-2014 10:24:42
ZYQ8TH	12/11/2014 10:24:42 (UTC-5)

TABLE 1

Question 23 - Applications

Consensus Result: No Consensus Reached

Expected Response Explanation:

No consensus was reached for question 23. Majority of the responses can be placed into one group with varying conversion differences. Variation seen for this question is due date and time conversions and response format. Below is a breakdown of the patterns seen in the responses given:

Unconverted response for this group can be found at:
root\data\com.android.chrome\app_chrome\Default\History

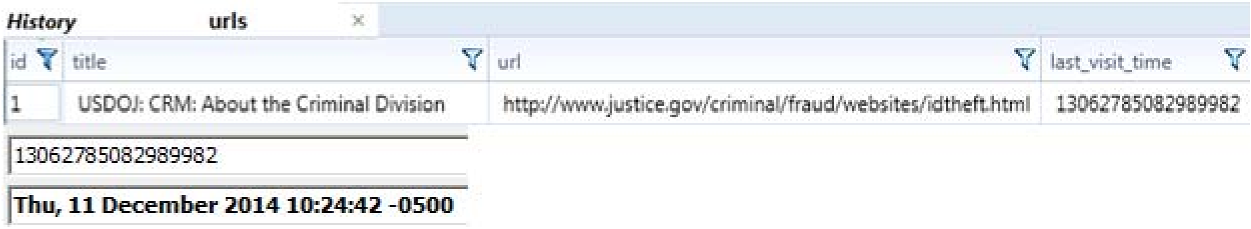
- 11-12-2014 10:24:42 – 21 participants
- 12-11-2014 10:24:42 – 6 participants
- 12-11-2014 15:24:42 – 1 participant
- 11-12-2014 15:24:42 – 2 participants

  -1 participants included local time of 11:24:42
- 12-11-2014 03:24:42

The expected response is asked for in dd-mm-yyyy format; however it is believed some participants reversed the order to mm-dd-yyyy. The time of the incident occurred during daylight savings time (GMT -5) therefore when the time is decoded from UTC to GMT -5 the time goes from 15:24:42 (3:24:42) to 10:24:42.

Information about Steve's browsing history in Chrome can be found in the History database. The urls table contains information about the web pages that Steve visited. The url with the id = 1 corresponds to the title "USDOJ:CRM: About the Criminal Division". Associated with this url is a timestamp for the last visit time. The timestamp is stored in a Google Chrome time format which must be converted into the requested time and date format. This file can be found at: root\data\com.android.chrome\app_chrome\Default\History

Expected Response Illustration:



id	title	url	last_visit_time
1	USDOJ: CRM: About the Criminal Division	http://www.justice.gov/criminal/fraud/websites/idtheft.html	13062785082989982

13062785082989982

Thu, 11 December 2014 10:24:42 -0500

TABLE 1

Question 24 - Applications

Question 24: In Google maps the suspect Steven Lefft requested driving directions to a bank. Provide the name of the bank.

Manufacturer's Expected Response: Capital One Bank

WebCode	Response
2HZNCM	Capitol One Bank
2MX9EK	Capital One Bank
2W2HLB	Capital One Bank
3JPC9M	Capital One
3UP3RA	Capitol One Bank
6GECZL	Capital One Bank
6HAU49	Capital One Bank
7TLJFH	Capital One Bank
9MAA37	Capitol One
ATTZ37	Capital One Bank - Patomac Run
BDWZNC	United Bank
EXQ8BW	Capital One Bank
EZFET9	United Bank
FFMX46	Capital One Bank
FHB8E7	Capital One Bank
H46R9T	Capital One Bank
H47R79	Capital One Bank
JVM7CV	Capital One Bank
LHAK2Z	Capital One Bank
LJ7ZDX	Capital one
NQYVN2	Capital One Bank
R6PT4T	Capital One
RECRVY	United Bank
RY2BNW	Capital One Bank
RYWRZT	Capital One Bank
TCHNEW	ATM (Capital One Bank)
UCCT9V	Capital One Bank - Potomac Run
UD8CCH	Capital One Bank
ULK4ZV	Capital One Bank
WLY9DQ	Capital One Bank [Timeline\#271\Web History]
XPRVJJ	Capital One Bank - Patomac Run
ZYQ8TH	Unable to locate Google map search.

TABLE 1

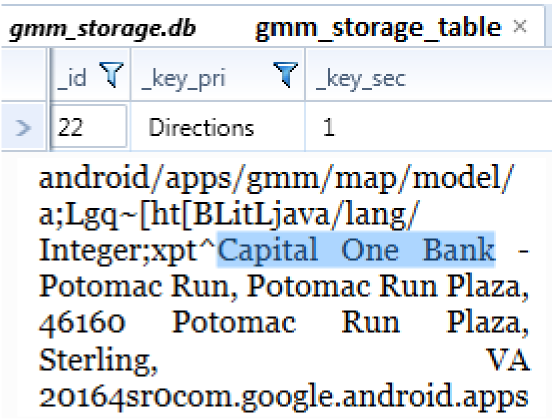
Question 24 - Applications

Consensus Result: Capital One Bank

Expected Response Explanation:

Information about Google maps activity can be found in the gmm_storage.db database. The gmm_storage_table table contains information about all of the activity on Google maps. One of the keys in that table is Directions. Associated with that key is a _data field that contains the information used to request driving directions to a bank. This file can be found at:
root\data\com.google.android.apps.maps\databases\gmm_storage.db

Expected Response Illustration:



_id	_key_pri	_key_sec
22	Directions	1

android/apps/gmm/map/model/
a;Lgq~[ht[BLitLjava/lang/
Integer;xpt^Capital One Bank -
Potomac Run, Potomac Run Plaza,
46160 Potomac Run Plaza,
Sterling, VA
20164sr0com.google.android.apps

TABLE 1

Question 25 - Applications

Question 25: The suspect Steven Lefft created an Outlook email account. What is the name associated with that account?

Manufacturer's Expected Response: Fund Scam

WebCode	Response
2HZNCM	Fund Scam
2MX9EK	Fund Scam
2W2HLB	Fund Scam
3JPC9M	Fund Scam
3UP3RA	Fund Scam
6GECZL	Fund Scam
6HAU49	Fund Scam
7TLJFH	Fund Scam
9MAA37	Fund Scam
ATTZ37	Fund Scam
BDWZNC	Fund Scam
EXQ8BW	Fund Scam
EZFET9	Fund Scam
FFMX46	Fund Scam
FHB8E7	Fund Scam
H46R9T	Fund Scam
H47R79	Fund Scam
JVM7CV	Fund Scam
LHAK2Z	Fund Scam
LJ7ZDX	Fund Scam
NQYVN2	Fund Scam
R6PT4T	Fund Scam
RECRVY	Fund Scam
RY2BNW	The setting listed Fund Scam. In the e-mail list it shows “Inheritance Foundation, in one of the e-mails it is addressed to Brian”.
RYWRZT	Brian "Fund Scam"
TCHNEW	Fund Scam
UCCT9V	Fund Scam
UD8CCH	Fund Scam
ULK4ZV	
WLY9DQ	"Brian" Inheritance Foundation is associated with this account per email Timestamp: 12/11/2014 08:51:32 PM
XPRVJJ	Fund Scam
ZYQ8TH	Fund Scam

TABLE 1

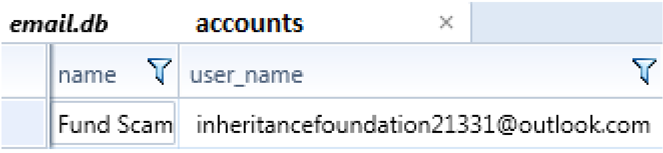
Question 25 - Applications

Consensus Result: Fund Scam

Expected Response Explanation:

Information about Steve’s email account can be found in the email.db database. The accounts table contains the email address along with the associated name for the email address.
This file can be found at: root\data\com.outlook.Z7\databases\email.db

Expected Response Illustration:



email.db accounts ×

name	user_name
Fund Scam	inheritancefoundation21331@outlook.com

TABLE 1

Question 26 - Applications

Question 26: What email address was used in the Outlook app?

Manufacturer's Expected Response: Inheritancefoundation21331@outlook.com

WebCode	Response
2HZNCM	inheritancefoundation21331@outlook.com
2MX9EK	inheritancefoundation21331@outlook.com
2W2HLB	inheritancefoundation21331@outlook.com
3JPC9M	inheritancefoundation21331@outlook.com
3UP3RA	inheritancefoundation21331@outlook.com
6GECZL	inheritancefoundation21331@outlook.com
6HAU49	inheritancefoundation21331@outlook.com
7TLJFH	inheritancefoundation21331@outlook.com
9MAA37	inheritancefoundation21331@outlook.com
ATTZ37	inheritancefoundation21331@outlook.com
BDWZNC	InheritanceFoundation21331@outlook.com
EXQ8BW	inheritancefoundation21331@outlook.com
EZFET9	inheritancefoundation21331@outlook.com
FFMX46	inheritancefoundation21331@outlook.com
FHB8E7	inheritancefoundation21331@outlook.com
H46R9T	inheritancefoundation21331@outlook.com
H47R79	inheritancefoundation21331@outlook.com
JVM7CV	inheritancefoundation21331@outlook.com
LHAK2Z	inheritancefoundation21331@outlook.com
LJ7ZDX	inheritancefoundation21331@outlook.com
NQYVN2	inheritancefoundation21331@outlook.com
R6PT4T	inheritancefoundation21331@outlook.com
RECRVY	inheritancefoundation21331@outlook.com
RY2BNW	inheritancefoundation21331@outlook.com
RYWRZT	inheritancefoundation21331@outlook.com
TCHNEW	Inheritancefoundation21331@outlook.com
UCCT9V	inheritancefoundation21331@outlook.com
UD8CCH	inheritancefoundation21331@outlook.com
ULK4ZV	inheritancefoundation21331@outlook.com
WLY9DQ	inheritancefoundation21331@outlook.com [Analyzed Data\ Emails]
XPRVJJ	inheritancefoundation21331@outlook.com
ZYQ8TH	inheritancefoundation21331@outlook.com

TABLE 1

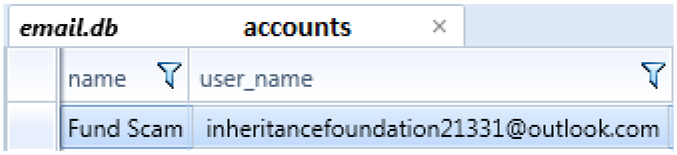
Question 26 - Applications

Consensus Result: Inheritancefoundation21331@outlook.com

Expected Response Explanation:

Information about Steve's Outlook email address can be found in the email.db database. The accounts table contains the user name Inheritancefoundation21331@outlook.com. This file can be found at: root\data\com.outlook.Z7\databases\email.db

Expected Response Illustration:



email.db accounts

name	user_name
Fund Scam	inheritancefoundation21331@outlook.com

TABLE 1

Question 27 - Communication

Question 27: What is the victim Harris Marvins' email address?

Manufacturer's Expected Response: harris.marvins@aol.com

WebCode	Response
2HZNCM	harris.marvins@aol.com
2MX9EK	harris.marvins@aol.com
2W2HLB	harris.marvins@aol.com
3JPC9M	harris.marvins@aol.com
3UP3RA	harris.marvins@aol.com
6GECZL	harris.marvins@aol.com
6HAU49	harris.marvins@aol.com
7TLJFH	harris.marvins@aol.com
9MAA37	harris.marvins@aol.com
ATTZ37	harris.marvins@aol.com
BDWZNC	harris.marvins@aol.com
EXQ8BW	harris.marvins@aol.com
EZFET9	harris.marvins@aol.com
FFMX46	harris.marvins@aol.com
FHB8E7	harris.marvins@aol.com
H46R9T	harris.marvins@aol.com
H47R79	harris.marvins@aol.com
JVM7CV	harris.marvins@aol.com
LHAK2Z	harris.marvins@aol.com
LJ7ZDX	harris.marvins@aol.com
NQYVN2	harris.marvins@aol.com
R6PT4T	harris.marvins@aol.com
RECRVY	harris.marvins@aol.com
RY2BNW	"Harris Marvins" <harris.marvins@aol.com>
RYWRZT	harris.marvins@aol.com
TCHNEW	“Harris Marvins” harris.marvins@aol.com
UCCT9V	harris.marvins@aol.com
UD8CCH	harris.marvins@aol.com
ULK4ZV	
WLY9DQ	harris.marvins@aol.com [Emails]
XPRVJJ	harris.marvins@aol.com
ZYQ8TH	harris.marvins@aol.com

TABLE 1

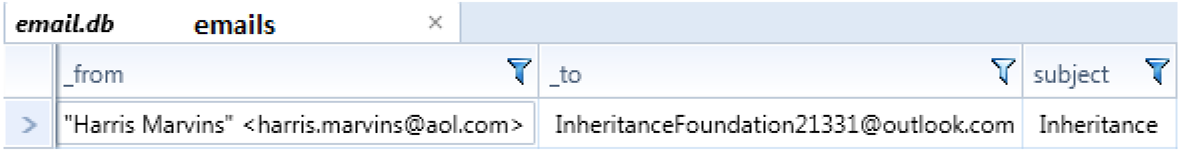
Question 27 - Communication

Consensus Result: harris.marvins@aol.com

Expected Response Explanation:

Information about Harris' email address can be found in the email.db database. In the emails table there is an email conversation between Steve and Harris. Harris' email address is harris.marvins@aol.com. This file can be found at: root\data\com.outlook.Z7\databases\email.db

Expected Response Illustration:



_from	_to	subject
"Harris Marvins" <harris.marvins@aol.com>	InheritanceFoundation21331@outlook.com	Inheritance

TABLE 1

Question 28 - Communication

Question 28: What is the subject of the email conversation between the suspect Steven Lefft and the victim Harris Marvins?

Manufacturer's Expected Response: Inheritance

WebCode	Response
2HZNCM	Inheritance
2MX9EK	Inheritance
2W2HLB	Inheritance
3JPC9M	Inheritance
3UP3RA	Inheritance
6GECZL	Inheritance
6HAU49	Inheritance
7TLJFH	Inheritance
9MAA37	Inheritance
ATTZ37	Inheritance
BDWZNC	Inheritance
EXQ8BW	Inheritance
EZFET9	Re: Inheritance
FFMX46	Inheritance
FHB8E7	Inheritance
H46R9T	Inheritance
H47R79	Inheritance
JVM7CV	Inheritance
LHAK2Z	Inheritance
LJ7ZDX	Inheritance
NQYVN2	Inheritance
R6PT4T	Inheritance
RECRVY	Inheritance
RY2BNW	Inheritance and Re: Inheritance
RYWRZT	Inheritance
TCHNEW	Re: Inheritance
UCCT9V	Inheritance
UD8CCH	Inheritance
ULK4ZV	
WLY9DQ	Subject: Inheritance [Emails]
XPRVJJ	Inheritance
ZYQ8TH	Inheritance

TABLE 1

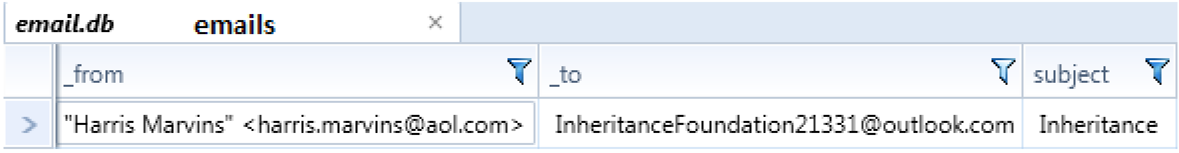
Question 28 - Communication

Consensus Result: Inheritance

Expected Response Explanation:

Information about Steve's Outlook emails can be found in the email.db database. The emails table shows an email conversation between Steve and Harris with the subject "Inheritance." This file can be found at: root\data\com.outlook.Z7\databases\email.db

Expected Response Illustration:



_from	_to	subject
"Harris Marvins" <harris.marvins@aol.com>	InheritanceFoundation21331@outlook.com	Inheritance

TABLE 1

Question 29 - Communication

Question 29: In the email conversation, the victim Harris Marvins sent the suspect Steven Lefft an attachment. What is the name of the attachment?

Manufacturer's Expected Response: SS.png

WebCode	Response
2HZNCM	SS.png
2MX9EK	SS.png
2W2HLB	SS.png
3JPC9M	SS.png
3UP3RA	ss.png
6GECZL	SS.png
6HAU49	SS.png
7TLJFH	SS.png
9MAA37	SS.png
ATTZ37	SS.png
BDWZNC	SS.png
EXQ8BW	SS.png
EZFET9	ss.png
FFMX46	SS.png
FHB8E7	SS.png
H46R9T	SS.png
H47R79	SS.png
JVM7CV	ss.png
LHAK2Z	ss.png
LJ7ZDX	SS.png
NQYVN2	SS.png
R6PT4T	SS.png
RECRVY	SS.png applicaton/png
RY2BNW	SS.png
RYWRZT	Anwar D Mogba
TCHNEW	SS.png
UCCT9V	SS.png
UD8CCH	SS.png
ULK4ZV	
WLY9DQ	Name of attachment = "SS_2331.png" Picutre of a Social Security card with the following info. In part, "123-45-6789...Anwar D Mogba..." a signature was also observed on picture. [Emails]
XPRVJJ	SS.png
ZYQ8TH	SS.png

TABLE 1

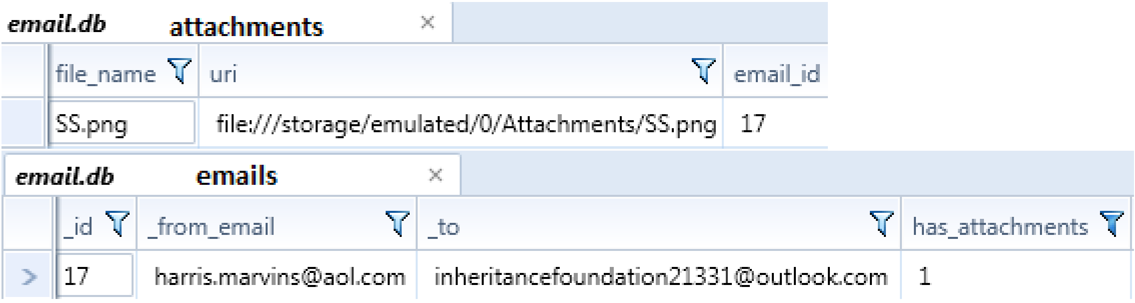
Question 29 - Communication

Consensus Result: SS.png

Expected Response Explanation:

Information about Steve's Outlook emails can be found in the email.db database. The attachments table shows one attachment with the file name "SS.png". This attachment corresponds to the email _id= 17 which is an email that Steve received from Harris. This file can be found at: root\data\com.outlook.Z7\databases\email.db

Expected Response Illustration:



file_name	uri	email_id
SS.png	file:///storage/emulated/0/Attachments/SS.png	17

_id	_from_email	_to	has_attachments
17	harris.marvins@aol.com	inheritancefoundation21331@outlook.com	1

TABLE 1

Question 30 - Communication

Question 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?

Manufacturer's Expected Response: $50 million dollars

WebCode	Response
2HZNCM	approximately $50 Million
2MX9EK	$50 Million
2W2HLB	$50 Million
3JPC9M	$50 Million
3UP3RA	$50 million
6GECZL	$50 million
6HAU49	$50 Million
7TLJFH	approximately $50 Million
9MAA37	$50 Million
ATTZ37	approximately $50 Million
BDWZNC	$50 Million
EXQ8BW	$50 million dollars
EZFET9	$50 Million Dollars
FFMX46	$50 million
FHB8E7	approximately 50 million
H46R9T	$50 million dollars
H47R79	$50 million dollars
JVM7CV	$ 50 million
LHAK2Z	$50 million
LJ7ZDX	$ 50 Million
NQYVN2	$50 Million
R6PT4T	$50 million
RECRVY	$50 million dollars
RY2BNW	Approximately $50 Million
RYWRZT	$50 million dollars
TCHNEW	$50 Million dollars
UCCT9V	$50 million dollars
UD8CCH	Approximately $50 Million
ULK4ZV	
WLY9DQ	Valued at $50 million dollars. Email stated the following in part, "…Mr. Mogba's remaning estate valued at $50 million dollars is legally yours…" [Emails]
XPRVJJ	approximately $50 Million
ZYQ8TH	$50 million

TABLE 1

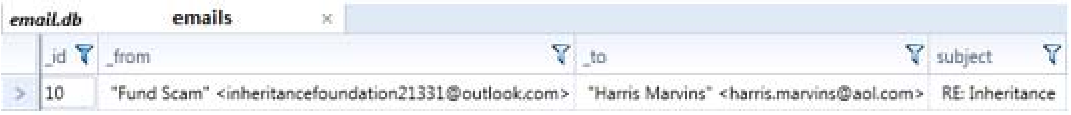
Question 30 - Communication

Consensus Result: $50 million dollars

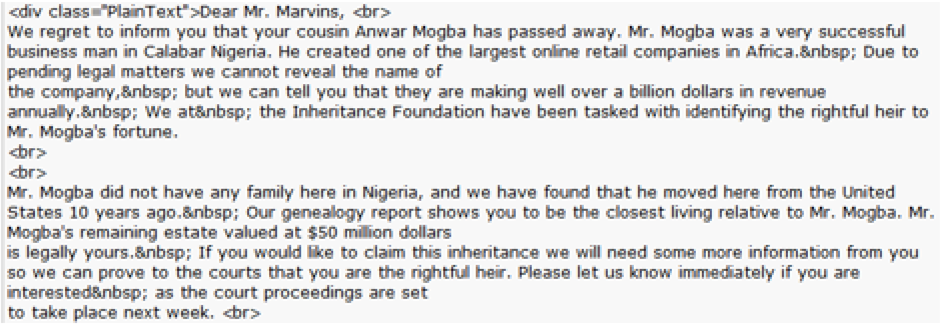
Expected Response Explanation:

Information about emails in outlook can be found in the email.db database. The emails table contains the content of all emails sent through the Outlook app. The email with _id = 10 contains a message where Steve tells Harris the estimated value of his cousin's estate. This file can be found at:
root\data\com.outlook.Z7\databases\email.db

Expected Response Illustration:



_id	_from	_to	subject
10	"Fund Scam" <inheritancefoundation21331@outlook.com>	"Harris Marvins" <harris.marvins@aol.com>	RE: Inheritance



```
<div class="PlainText">Dear Mr. Marvins, <br>
We regret to inform you that your cousin Anwar Mogba has passed away. Mr. Mogba was a very successful
business man in Calabar Nigeria. He created one of the largest online retail companies in Africa.&nbsp; Due to
pending legal matters we cannot reveal the name of
the company,&nbsp; but we can tell you that they are making well over a billion dollars in revenue
annually.&nbsp; We at&nbsp; the Inheritance Foundation have been tasked with identifying the rightful heir to
Mr. Mogba's fortune.
<br>
<br>
Mr. Mogba did not have any family here in Nigeria, and we have found that he moved here from the United
States 10 years ago.&nbsp; Our genealogy report shows you to be the closest living relative to Mr. Mogba. Mr.
Mogba's remaining estate valued at $50 million dollars
is legally yours.&nbsp; If you would like to claim this inheritance we will need some more information from you
so we can prove to the courts that you are the rightful heir. Please let us know immediately if you are
interested&nbsp; as the court proceedings are set
to take place next week. <br>
```

TABLE 1

Question 31 - Communication

Question 31: Did the suspect Steven Lefft ever text message the victim Harris Marvins?

Manufacturer's Expected Response: Yes

WebCode	Response
2HZNCM	Yes
2MX9EK	Yes
2W2HLB	Yes
3JPC9M	Yes
3UP3RA	Yes.
6GECZL	Yes
6HAU49	Yes
7TLJFH	Yes
9MAA37	Yes (MMS)
ATTZ37	Yes
BDWZNC	Yes
EXQ8BW	Yes
EZFET9	Yes
FFMX46	Yes
FHB8E7	Yes
H46R9T	1 time via MMS
H47R79	Yes
JVM7CV	Yes
LHAK2Z	Yes, mms message
LJ7ZDX	Yes (10-12-2014 at 13:23:58 hours)
NQYVN2	Yes
R6PT4T	Yes
RECRVY	Yes. Greetings Mr. Marvins this message is to inform you that there is a large sum of money that is in your name and is unclaimed. For more information please contact inheritancefoundation21331@outlook.com immediately.
RY2BNW	Yes
RYWRZT	Yes (MMS message)
TCHNEW	Yes
UCCT9V	A text message in the form of an MMS was sent from Steven Lefft to Harris Marvins on 10-12-2014 13:23:58 (GMT-5).
UD8CCH	Yes. He sent an MMS.
ULK4ZV	
WLY9DQ	Yes- An MMS message was observed an attachment marked in part, "Greetings Mr. Marvins… "sent to 5712129673 Harris [MMS Message\#4\12/10/2014…Harris] & noted contacts Name Harris Mobile 5712129673 [Contacts]
XPRVJJ	Yes
ZYQ8TH	No

TABLE 1

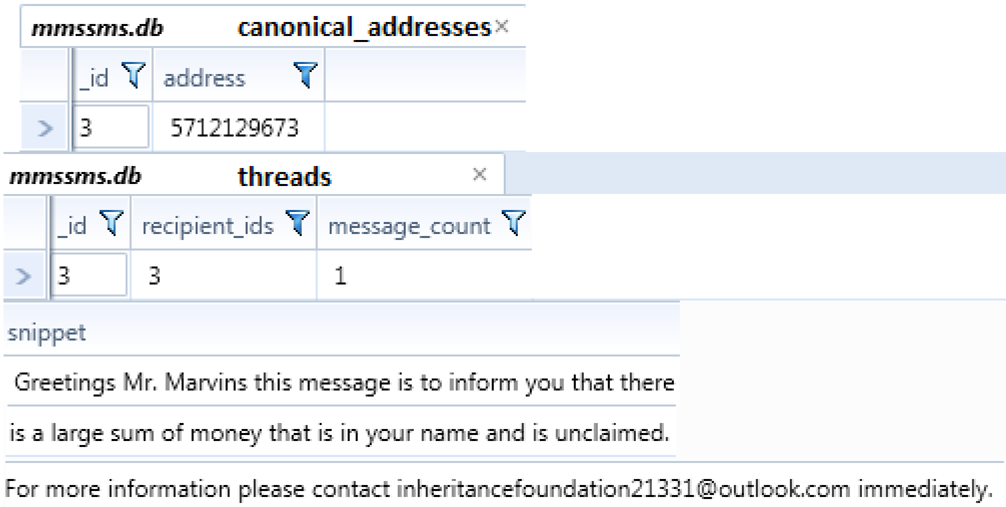
Question 31 - Communication

Consensus Result: Yes

Expected Response Explanation:

Information about text messages can be found in the mmssms.db database. The canonical_addresses table contains the phone number associated with each conversation thread. Harris' phone number corresponds to _id = 3. The threads table contains information about each conversation thread. Thread _id= 3 contains a message addressed to Mr. Marvins. This file can be found at: root\data\com.android.providers.telephony\databases\mmssms.db

Expected Response Illustration:



_id	address
3	5712129673

_id	recipient_ids	message_count
3	3	1

snippet
Greetings Mr. Marvins this message is to inform you that there is a large sum of money that is in your name and is unclaimed. For more information please contact inheritancefoundation21331@outlook.com immediately.

TABLE 1

Question 32 - Communication

Question 32: What is the filename of the attachment that the suspect Steven Lefft sent Paul through text message?

Manufacturer's Expected Response: 20141211_140829.jpeg

WebCode	Response
2HZNCM	20141211_140829.jpeg
2MX9EK	20141211_140829.jpeg
2W2HLB	20141211_140829.jpeg
3JPC9M	smil.xml text_0.txt
3UP3RA	20141211_140829.jpeg
6GECZL	20141211_140829.jpeg
6HAU49	20141211_140829.jpeg
7TLJFH	text_0.txt
9MAA37	20141211_140829.jpeg
ATTZ37	20141211_140829.jpeg
BDWZNC	20141211_140829.jpeg
EXQ8BW	20141211_140829.jpeg
EZFET9	20141211_140829.jpeg
FFMX46	20141211_140829.jpeg
FHB8E7	20141211_140829.jpeg
H46R9T	20141211_140829.jpeg
H47R79	20141211_140829.jpeg
JVM7CV	20141211_140829.jpg
LHAK2Z	20141211_140829.jpeg
LJ7ZDX	20141211_140829.jpeg
NQYVN2	20141211_140829.jpeg
R6PT4T	20141211_140829.jpeg
RECRVY	20141211_140829.jpeg
RY2BNW	20141211_140829.jpeg
RYWRZT	5127 (20141211_140829.jpeg)
TCHNEW	20141211_140829.jpeg
UCCT9V	20141211_140829.jpeg
UD8CCH	20141211_140829.jpeg
ULK4ZV	
WLY9DQ	Filename= 20141211_140829_5127.jpeg [MMS\#2\12/11/2014 11:35:08 AM\...Paul]
XPRVJJ	20141211_140829.jpeg
ZYQ8TH	20141211_140829.jpeg

TABLE 1

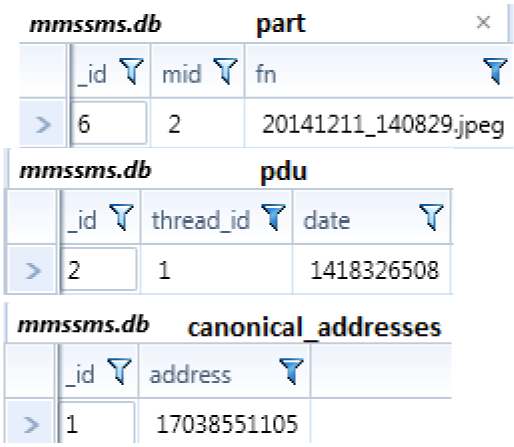
Question 32 - Communication

Consensus Result: 20141211_140829.jpeg

Expected Response Explanation:

Information about text messages can be found in the mmssms.db database. The part table contains information about what attachment files were sent. The fn field contains the name of the attachment. The mid field contains a key that corresponds to the _id field in the pdu table. The pdu table contains a thread_id field. This field is used to identify the messaging thread. The thread_id corresponds to _id in the canonical_addresses table. The canonical_addresses table contains the numbers that correspond to each thread partner. In the canonical_addresses table where _id=1, the corresponding number is 17038551105. This is Paul's number. Thus the attachment titled '20141211_140829.jpeg' was sent to Paul. The mmssms.db database can be found at: root\data\com.android.providers.telephony\databases\mmssms.db

Expected Response Illustration:



mmssms.db part

_id	mid	fn
6	2	20141211_140829.jpeg

mmssms.db pdu

_id	thread_id	date
2	1	1418326508

mmssms.db canonical_addresses

_id	address
1	17038551105

TABLE 1

Question 33 - Communication

Question 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)

Manufacturer's Expected Response: 10-12-2014 11:02:31

WebCode	Response
2HZNCM	10-12-2014 11:02:31
2MX9EK	10-12-2014 (10 Dec 2014) 11:02:31
2W2HLB	12-10-2014 11:02:31
3JPC9M	12-10-2014 16:02:31
3UP3RA	12-10-2014 11:02:31
6GECZL	10-12-2014 11:02:31 AM
6HAU49	10-12-2014 11:02:31
7TLJFH	10-12-2014 11:02:31
9MAA37	10-12-2014 11:02:31
ATTZ37	10-12-2014 11:02:31
BDWZNC	10-12-2014 11:02:31 GMT-0500
EXQ8BW	12-10-2014 11:02:31
EZFET9	12-10-2014 11:02:31
FFMX46	10-12-2014 11:02:31
FHB8E7	10/12/2014 11:02:31 AM (UTC-5)
H46R9T	10/12/2014 16:02
H47R79	10-12-2014 11:02:31
JVM7CV	10-12-2014 / 16:02:31 (UTC+0) // 10-12-2014 / 12:02:31 (local time)
LHAK2Z	10-12-2014 (10-Dec-2014)/11:02:31
LJ7ZDX	10-12-2014 at 11:02:31 hours
NQYVN2	10-12-2014 11:02:31 -0500
R6PT4T	10-12-2014 11:02:31
RECRVY	12/11/2014 12:16:29 PM(UTC-5)
RY2BNW	10-12-2014 11:02:31 hrs
RYWRZT	12/10/2014 04:02:31
TCHNEW	10/12/2014 11:02:31 AM(UTC-5) dec 10 2014
UCCT9V	10-12-2014 11:02:31(UTC-5)
UD8CCH	10-12-2014 11:02:31 (GMT - 05:00)
ULK4ZV	
WLY9DQ	10/12/2014 11:02:31 AM (UTC-5) using the phone and not 3rd party application. [Call Log\#8\7038551105 Paul\1:09 9duration)]
XPRVJJ	10-12-2014 11:02:31
ZYQ8TH	12/10/2014 11:02:31 (UTC-5)

TABLE 1

Question 33 - Communication

Consensus Result: No Consensus Reached

Expected Response Explanation:

No consensus was reached for question 33. Majority of the responses can be placed into one group with varying conversion differences. Variation seen for this question is due to date and time conversions and response format. Below is a breakdown of the patterns seen in the responses given:

Unconverted response for this group can be found at:
root\data\com.sec.android.provider.logsprovider\databases\logs.db

- 10-12-2014 11:02:31 – 21 participants
- 12-10-2014 11:02:31 – 5 participants
- 10-12-2014 16:02:31 – 2 participants

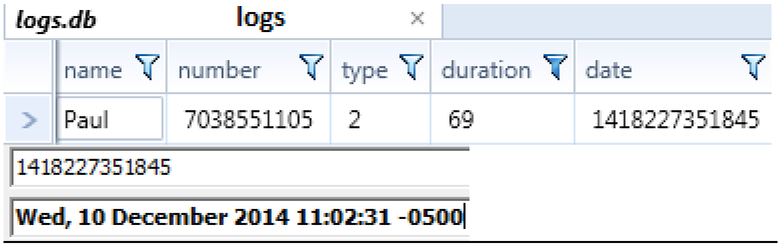
-1 participant included 12:02:31 as local time

- 12-10-2014 04:02:31

The expected response is asked for in dd-mm-yyyy format; however it is believed some participants reversed the order to mm-dd-yyyy. This conversion creates great variation in the responses. The time of the incident occurred during daylight savings time (GMT -5) therefore when the time is decoded from UTC to GMT -5 the time goes from 16:02:31 (04:02:31) to 11:02:31.

Information on Steve's call to Paul can be found in the logs.db database under the logs table. In the logs table an event was logged to the phone number 7038551105, with the name Paul, the value listed for this event is 2 signifying that it is outgoing, and it contains a value for duration signifying that it was a call. The date field contains a Unix Epoch time format associated with the call which must be converted into the requested time and date format. The logs.db database can be found at:
root\data\com.sec.android.provider.logsprovider\databases\logs.db

Expected Response Illustration:



logs.db logs

name	number	type	duration	date
Paul	7038551105	2	69	1418227351845

1418227351845

Wed, 10 December 2014 11:02:31 -0500

10-12-2014 11:02:31

TABLE 1

Question 34 - Communication

Question 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)

Manufacturer's Expected Response: 11-12-2014 10:43:40

WebCode	Response
2HZNCM	11-12-2014 10:43:40
2MX9EK	11-12-2014 (11 Dec 2014) 10:43:40
2W2HLB	12-11-2014 10:43:40
3JPC9M	12-11-2014 15:43:40
3UP3RA	12-11-2014 10:43:40
6GECZL	11-12-2014 10:43:40 AM
6HAU49	11-12-2014 10:43:40
7TLJFH	11-12-2014 10:43:40
9MAA37	11-12-2014 10:43:40
ATTZ37	11-12-2014 10:43:40
BDWZNC	11-12-2014 10:43:40 GMT-0500
EXQ8BW	12-11-2014 10:43:40
EZFET9	12-11-2014 10:43:40
FFMX46	11-12-2014 10:43:40
FHB8E7	11/12/2014 10:43:40 AM (UTC-5)
H46R9T	11/12/2014 15:43
H47R79	11-12-2014 10:43:40
JVM7CV	11-12-2014 / 17:15:58 (UTC+0) // 11-12-2014 / 13:15:58 (local time)
LHAK2Z	11-12-2014 (11-Dec-2014)/10:43:40
LJ7ZDX	11-12-2014 at 10:43:40 hours
NQYVN2	11-12-2014 10:43:40 -0500
R6PT4T	11-12-2014 10:43:40
RECRVY	12/11/2014 10:43:40 AM(UTC-5)
RY2BNW	11-12-2014 10:43:40 hrs
RYWRZT	12/11/2014 03:43:40
TCHNEW	11/12/2014 10:43:40 AM(UTC-5) dec 11 2014
UCCT9V	11-12-2014 10:43:40(UTC-5)
UD8CCH	11-12-2014 10:43:40 (GMT - 05:00)
ULK4ZV	
WLY9DQ	11/12/2014 10:43:40 AM (UTC-5) = time stamp for missed call [Call Log\Missed]
XPRVJJ	11-12-2014 10:43:40
ZYQ8TH	12/11/2014 10:43:40 (UTC-5)

TABLE 1

Question 34 - Communication

Consensus Result: No Consensus Reached

Expected Response Explanation:

No consensus was reached for question 34. Majority of the responses can be placed into one group with varying conversion differences. Variation seen for this question is due to date and time conversions and response format. Below is a breakdown of the patterns seen in the responses given:

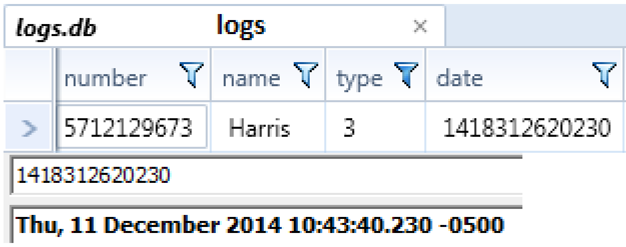
Unconverted response for this group can be found at:
root\data\com.sec.android.provider.logsprovider\databases\logs.db

- 11-12-2014 10:43:40 – 21 participants
- 12-11-2014 10:43:40 – 6 participants
- 12-11-2014 15:43:40 – 1 participant
- 11-12-2014 15:43: -1 participant
- 12-11-2014 03:43:40 -1 participant

The expected response is asked for in dd-mm-yyyy format; however it is believed some participants reversed the order to mm-dd-yyyy. This conversion creates great variation in the responses. The time of the incident occurred during daylight savings time (GMT -5) therefore when the time is decoded from UTC to GMT -5 the time goes from 15:43:40 (03:43:40) to 10:43:40.

Information on Steve's missed call from Harris can be found in the logs.db database under the logs table. In the logs table an event was logged to the phone number 5712129673, with the name Harris, the value listed for this event is 3 signifying that it was missed. There is a timestamp associated with the call in a Unix Epoch time format which must be converted into the requested time and date format. This file can be found at: root\data\com.sec.android.provider.logsprovider\databases\logs.db

Expected Response Illustration:



number	name	type	date
5712129673	Harris	3	1418312620230

1418312620230

Thu, 11 December 2014 10:43:40.230 -0500

TABLE 1

Question 35 - Communication

Question 35: What is the content of the last text message that the suspect Steven Lefft sent to Paul?

Manufacturer's Expected Response: Of course I did. We're gonna be rich brother!

WebCode	Response
2HZNCM	Of course I did. We’re gonna be rich brother!
2MX9EK	Of course I did. We're gonna be rich brother!
2W2HLB	Of course I did. We're gonna be rich brother!
3JPC9M	Of course I did. We're gonna be rich brother!
3UP3RA	Of course I did. We're gonna be rich brother!
6GECZL	Of course I did. We're gonna be rich brother!
6HAU49	Of course I did. We're gonna be rich brother!
7TLJFH	Of course I did. We're gonna be rich brother!
9MAA37	Of course I did. We're gonna be rich brother!
ATTZ37	Of course I did. We're gonna be rich brother!
BDWZNC	Of course I did. We're gonna be rich brother!
EXQ8BW	Of course I did. We're gonna be rich brother!
EZFET9	This ones name is Harris Marvins
FFMX46	Of course I did. We're gonna be rich brother!
FHB8E7	The message answered a received message with yes, he used a fake name, and stated, "we're gonna be rich brother!".
H46R9T	" Of course I did. We're gonna be rich brother!"
H47R79	Of course I did. We're gonna be rich brother!
JVM7CV	Of course I did. We're gonna be rich brother!
LHAK2Z	They are going to be rich, "We're gonna be rich brother?"
LJ7ZDX	Of course I did. We´re gonna be rich brother!
NQYVN2	Of course I did. We're gonna be rich brother!
R6PT4T	Of course I did. We're gonna be rich brother!
RECRVY	Found the post office we can use
RY2BNW	Of course I did. We're gonna be rich brother!
RYWRZT	Of course I did. We're gonna be rich brother!
TCHNEW	Of course I did. We're gonna be rich brother!
UCCT9V	Of course I did. We're gonna be rich brother!
UD8CCH	Of course I did. We're gonna be rich brother!
ULK4ZV	
WLY9DQ	Content of last text message = "Of course I did. We're gonna be rich brother!" date stamp =12/11/2014 4:17:42 PM (UTC-5) [SMSMessages\Sent]
XPRVJJ	Of course I did. We're gonna be rich brother!
ZYQ8TH	Of course I did. We're gonna be rich brother!

TABLE 1

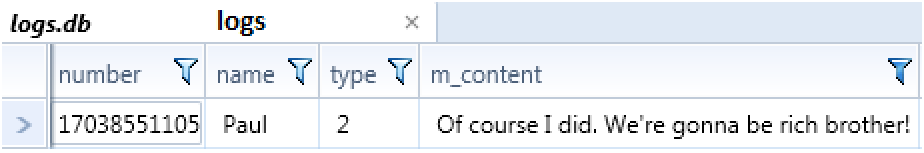
Question 35 - Communication

Consensus Result: Of course I did. We're gonna be rich brother!

Expected Response Explanation:

Information about text messages and calls can be found in the logs.db database. The logs table contains information about calls and messaging events. The last event stored is an outgoing text to Paul. This is demonstrated as the value for the type field is 2 signifying that it is outgoing and the name of the recipient is Paul. This file can be found at: root\data\com.sec.android.provider.logsprovider\databases\logs.db

Expected Response Illustration:



number	name	type	m_content
17038551105	Paul	2	Of course I did. We're gonna be rich brother!

TABLE 1

Question 36 - Communication

Question 36: How many Viber calls occurred between the suspect Steven Lefft and Paul? (Include calls with 0 duration)

Manufacturer's Expected Response: 5

WebCode	Response
2HZNCM	5
2MX9EK	5
2W2HLB	4
3JPC9M	5
3UP3RA	4
6GECZL	4
6HAU49	5
7TLJFH	5
9MAA37	4
ATTZ37	5
BDWZNC	5
EXQ8BW	4
EZFET9	4
FFMX46	5
FHB8E7	5
H46R9T	5 times
H47R79	5 calls
JVM7CV	5
LHAK2Z	5
LJ7ZDX	7 (Seven)
NQYVN2	Five (5)
R6PT4T	4
RECRVY	Two
RY2BNW	Five
RYWRZT	(4) 12/11/2014 01:33:17 45 sec, 12/11/2014 05:15:58 00 sec, 12/11/2014 05:16:11 00 sec, 12/11/2014 05:16:29 54 sec
TCHNEW	Five
UCCT9V	5
UD8CCH	Five (05)
ULK4ZV	
WLY9DQ	4 calls using Viber based on Call Log [Call Log]
XPRVJJ	5
ZYQ8TH	4

TABLE 1

Question 36 - Communication

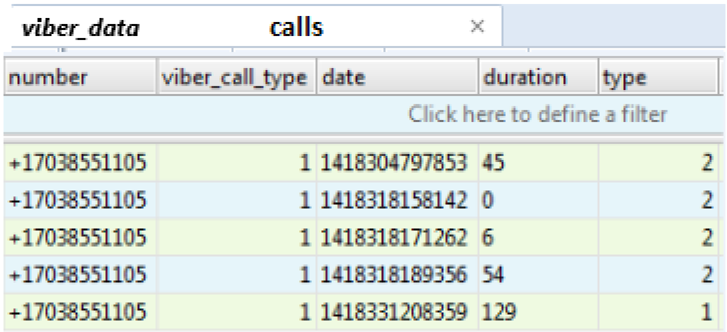
Consensus Result: No consensus reached

Expected Response Explanation:

The viber_data database shows that five (5) calls were recorded by the viber application between Steve and Paul. Four (4) of the calls were outgoing (as indicated in the database "type" with a "2"), one of the calls was incoming (as indicated in the database "type" with a "1"). Due to the ambiguity of the question both responses of four (4) and five (5) are representative of calls that were recorded between Steve and Paul.

Information about Viber calls can be found in the viber_data database. Under the calls table there are 5 calls to Paul’s number. This file can be found at: root\data\com.viber.voip.\databases\viber_data

Expected Response Illustration:



number	viber_call_type	date	duration	type
+17038551105	1	1418304797853	45	2
+17038551105	1	1418318158142	0	2
+17038551105	1	1418318171262	6	2
+17038551105	1	1418318189356	54	2
+17038551105	1	1418331208359	129	1

TABLE 1

Question 37 - Communication

Question 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)

Manufacturer's Expected Response: 11-12-2014 15:53:28

WebCode	Response
2HZNCM	11-12-2014 20:53:28hrs
2MX9EK	11-12-2014 (11-Dec-2014) 14:53:28
2W2HLB	12-11-2014 12:16:29
3JPC9M	12-11-2014 17:16:29
3UP3RA	12-11-2014 12:16:29
6GECZL	11-12-2014 8:33:17
6HAU49	11-12-2014 15:53:28
7TLJFH	11-12-2014 12:16:29
9MAA37	11-12-2014 12:16:29
ATTZ37	11-12-2014 15:53:28
BDWZNC	11-12-2014 15:53:28 GMT-0500
EXQ8BW	12-11-2014 12:16:29
EZFET9	12-11-2014 12:16:29
FFMX46	11-12-2014 15:53:28
FHB8E7	11/12/2014 15:53:28 (UTC-5)
H46R9T	Time stamp (UTC): 11/12/2014 20:53:28
H47R79	11-12-2014 15:53:28
JVM7CV	11-12-2014 / 20:53:28(UTC+0) // 11-12-2014 / 16:53:28(local time)
LHAK2Z	11-12-2014 (11-Dec-2014)/15:53:28
LJ7ZDX	11-12-2014 at 21:53:18 hours
NQYVN2	11-12-2014 15:53:28 -0500
R6PT4T	11-12-2014 12:16:29
RECRVY	12/11/2014 12:16:29
RY2BNW	11-12-2014 15:53:28
RYWRZT	12/11/2014 05:16:29
TCHNEW	11/12/2014 15:53:28.359 -0500 (UTC-5) dec 11, 2014
UCCT9V	11-12-2014 15:53:28 (UTC-5)
UD8CCH	11-12-2014 15:53:28 (GMT - 05:00)
ULK4ZV	11-12-2014 15:53:28
WLY9DQ	Las Viber call= 11/12/2014 12:16:29 PM (UTC-5) Duration= 00:00:54 [Call Log]
XPRVJJ	11-12-2014 15:53:28
ZYQ8TH	12/11/2014 12:16:29 (UTC-5)

TABLE 1

Question 37 - Communication

Consensus Result: No consensus reached

Expected Response Explanation:

No consensus was reached for question 37. Majority of the responses can be placed in groups based on similar patterns. Variation seen for this question is due to location examiner pulled the data from and date/time conversions. Below is a breakdown of the patterns seen in the responses given:

Unconverted response for this group can be found at: root\data\com.viber.voip.\databases\viber_data – calls table

- 11-12-2014 15:53:28 – 15 participants
- 11-12-2014 14:53:28 – 1 participant
- 11-12-2014 20:53:28 – 3 participants

-1 participant reported 16:53:28 as local time

- 11-12-2014 21:53:18 – 1 participant

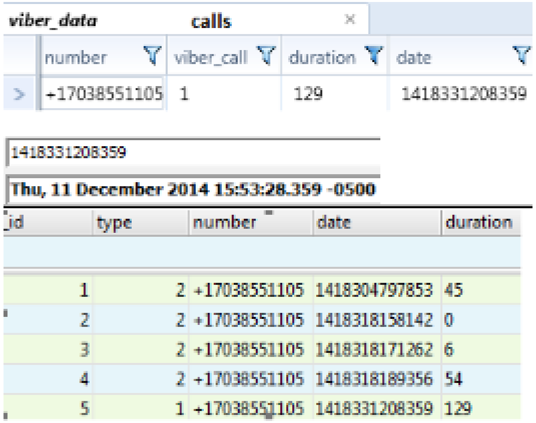
Unconverted response for this group can be found at: root\data\com.viber.voip.\databases\viber_data – calls table; it can also be the last call reported by a tool used:

- 11-12-2014 12:16:29 – 3 participants
- 12-11-2014 12:16:29 – 6 participants
- 12-11-2014 05:16:29 – 1 participant
- 12-11-2014 17:16:29 – 1 participant

Ambiguity in the question asked also produced a variation in the answers provided. There are a total of five calls that occur using the Viber application. Four of those calls are "outgoing" calls and one is an "incoming" call. These five calls can be seen in the following path: root\data\com.viber.voip.\databases\viber_data. During analysis and validation of the exam, we noted that some tools only report the four outgoing calls in the Viber artifacts. Majority of participants answered that the call on 11-12-2014 at 15:53:28 was the last call. However, other participants identified the last outgoing call, 12:16:29 on 11-12-2014. The expected response was looking for the last call to take place using the Viber application, although some tools may have reported the last outgoing call as the last call.

Information about Viber calls can be found in the viber_data database. In the calls table there are 5 calls to Paul's number along with a date field that contains a timestamp of when the call occurred. The timestamp is stored in a Unix Epoch time format which must be converted into the requested time and date format. This file can be found at: root\data\com.viber.voip.\databases\viber_data

Expected Response Illustration:



number	viber_call	duration	date
+17038551105	1	129	1418331208359

1418331208359

Thu, 11 December 2014 15:53:28.359 -0500

id	type	number	date	duration
1	2	+17038551105	1418304797853	45
2	2	+17038551105	1418318158142	0
3	2	+17038551105	1418318171262	6
4	2	+17038551105	1418318189356	54
5	1	+17038551105	1418331208359	129

TABLE 1

Question 38 - Communication

Question 38: What is the last message that the suspect Steven Lefft sent to Paul in the Viber app.

Manufacturer's Expected Response: Pretty good sounds quality

WebCode	Response
2HZNCM	Pretty good sounds quality
2MX9EK	Pretty good sounds quality
2W2HLB	Pretty good sounds quality
3JPC9M	It looks like we got him. Fingers crossed
3UP3RA	Pretty good sounds quality
6GECZL	Pretty good sounds quality
6HAU49	It looks like we got him. Fingers crossed
7TLJFH	Pretty good sounds quality
9MAA37	It looks like we got him. Fingers crossed
ATTZ37	It looks like we got him. Fingers crossed
BDWZNC	Pretty good sounds quality
EXQ8BW	Pretty good sounds quality
EZFET9	of course I did we're gonna be rich brother!
FFMX46	Pretty good sounds quality
FHB8E7	"it looks like we got him. Fingers crossed."
H46R9T	"It looks like we got him. Fingers crossed"
H47R79	Pretty good sounds quality
JVM7CV	11/12/2014 / 13:36:23(UTC+0) // 11/12/2014 / 9:36:23(local time)
LHAK2Z	"It looks like we got him. Fingers crossed"
LJ7ZDX	Pretty good sounds quality
NQYVN2	Pretty good sounds quality
R6PT4T	It looks like we got him. Fingers crossed
RECRVY	It looks like we got him. Fingers crossed
RY2BNW	Pretty good sounds quality
RYWRZT	Pretty good sounds quality
TCHNEW	Pretty good sounds quality
UCCT9V	Pretty good sounds quality
UD8CCH	Pretty good sounds quality
ULK4ZV	Pretty good sounds quality
WLY9DQ	Last Viber app message= "Pretty good sounds quality" Steve L 12/11/2014 8:36:23 AM (UTC -5) [Chats\Viber]
XPRVJJ	It looks like we got him. Fingers crossed
ZYQ8TH	Pretty good sounds quality

TABLE 1

Question 38 - Communication

Consensus Result: No consensus reached

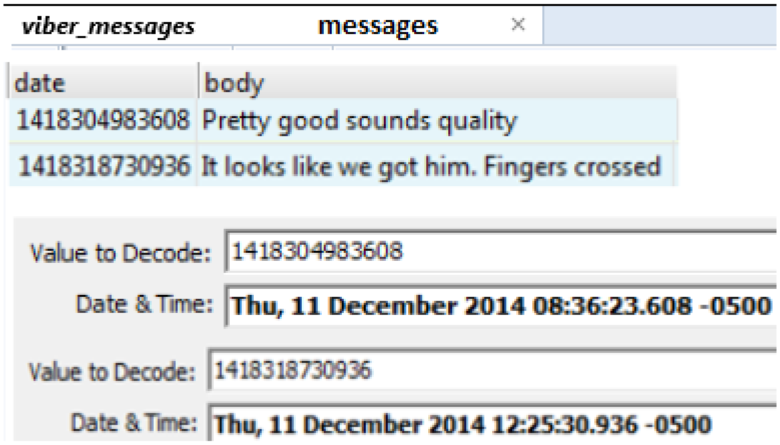
Expected Response Explanation:

Ambiguity in the question asked produced variation in the responses provided. The last messages to be exchanged between Steve and Paul via Viber is “It looks like we got him. Fingers crossed.” However, the question asks for the last message the suspect Steve sent to Paul; “Pretty good sounds quality.” Below is a breakdown of the variation in responses:

- Pretty good sounds quality – 20 participants
- It looks like we got him. Finger crossed. – 10 participants

Information about messages sent through the Viber app can be seen in the viber_messages database. This file can be found at: root\data\com.viber.voip\databases\viber_messages

Expected Response Illustration:



date	body
1418304983608	Pretty good sounds quality
1418318730936	It looks like we got him. Fingers crossed

Value to Decode: 1418304983608

Date & Time: Thu, 11 December 2014 08:36:23.608 -0500

Value to Decode: 1418318730936

Date & Time: Thu, 11 December 2014 12:25:30.936 -0500

TABLE 1

Question 39 - Communication

Question 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?

Manufacturer's Expected Response: George Trews

WebCode	Response
2HZNCM	George Trews
2MX9EK	George Trews
2W2HLB	George Trews
3JPC9M	George Trews
3UP3RA	George Trews
6GECZL	George Trews
6HAU49	George Trews
7TLJFH	George Trews
9MAA37	George Trews
ATTZ37	George Trews
BDWZNC	George Trews
EXQ8BW	George Trews
EZFET9	George Trews
FFMX46	George Trews
FHB8E7	George Trews
H46R9T	George Trews
H47R79	George Trews
JVM7CV	George Trews
LHAK2Z	George Trews
LJ7ZDX	George Trews
NQYVN2	George Trews
R6PT4T	George Trews
RECRVY	George Trews
RY2BNW	George Trews is gonna be the target for our next scam
RYWRZT	George Trews
TCHNEW	George Trews
UCCT9V	George Trews
UD8CCH	George Trews
ULK4ZV	
WLY9DQ	George Trews [SMS Messages\Inbox] The message was timestamp 12/11/204 4:15:53 PM (UTC-5) from Paul with body message stating "George Trews is gonna be the target for our next scam"
XPRVJJ	George Trews
ZYQ8TH	George Trews

TABLE 1

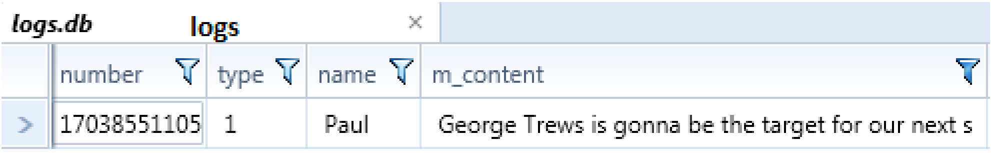
Question 39 - Communication

Consensus Result: George Trews

Expected Response Explanation:

Information about text messages and calls can be found in the logs.db database. The logs table contains information about calls and messaging events. In the logs table there is a text message from the conversation with Paul where a new target is identified. This text message has the value 1 for its type signifying that it is an incoming message. This file can be found at:
root\data\com.sec.android.provider.logsprovider\databases\logs.db

Expected Response Illustration:



number	type	name	m_content
17038551105	1	Paul	George Trews is gonna be the target for our next s

Additional Comments

TABLE 2

WebCode	Additional Comments
2HZNCM	Several of the questions left some interpretation of what actually was being requested. It appeared more like a competancy test than a proficiency test. The complication leads to longer exam time and spending days on a proficiency exam is not what is needed. The wording is confusing and caused the additional time.. like the use of; "last" when there is only one.."attempt" when there is no fail/success log to review. The first url visited is always, welcome/chrome.html. I must be missing a specific log for Viber to show app launch. There are several modified dates from the 12/12 but they show in crash analytics and last modified database. The comm log for Viber show successful converstations, but doesn't address the possibility of just opening the app and viewing. So, I went with the last db modified date. When asking for banking directions, it was pretty confusing to see three map.google.com searches. Having to narrow down to final destination, "turn by" directions took some time. Having to transcibe the dates into a dd-mm-yyyy can also be confusing, as most of us always use mm-dd-yyyy. The test also had lots of old data from activity 6mo prior. This can be confusing during the test process when none of the information is requested for this test.
2W2HLB	For question # 2 there are 2 answers provided because the specific type of SHA1 value was not clarified in the question. The 2 values provided are the most common types, in my experience, utilized in this field. Responses to this test were given based on the clarity of the questions. In actual case work the requesting entity would have been contacted.
3JPC9M	Investigative Leads: Possible co-conspirators: - Paul Gee - Facebook Display Name: Paul Gee - Android Contact: Paul -lefty21331@gmail.com - leftout21331@yahoo.com - inheritancefoundation21331@outlook.com - (703) 855-1105 - Shawn Tellford - Skype username: live.shawntell4rd - Jordan m - Skype username: likejordan21331 App Usernames: - Skype usernames: pcot21331 kelli.lasher1 - Viber username: Steve L - Snapchat username: incognito21331 Possible other scams: - Fraud - Kidnapping
3UP3RA	The responses to the test are based on the clarity of the request. In actual case work, any needed clarity would have been requested from the entity requesting the forensic exam. The SHA1 value to question 1 is the base32. As this wasn't clear in the question, I went to the default value for my software.
9MAA37	Question 24: I recovered what I think is the mytracks.db this has two entries in it one called "Surveillance" with description Spying on the target and the second was named "Abduction" with the description picking up the target. Theses where both in the category driving. However where not directly related to a bank the second one end of journey was close to a Citibank ATM. Findings for the answer i gave as Capitol One where based on audio files giving directions to capitol one located in the com.google.apps.maps directory, and secondly recovered data from the gmm_storage.db
EXQ8BW	It should be noted that the answers provided to the questions listed are based on the questioned asked in the manner in which they were asked. At times the questions were not clear on what information they were seeking. Also some questions appear to offer formatting examples for answers, but they DO NOT specifically request that the answer be provided in that certain format. Had this been a real world case, I would have contacted the case detective and sought clarification on the information requested, when clarification was needed.
EZFET9	Question 6- The phone last powered on on 12/12/14 at 9:15 AM. The phone was powered on and then powered off 6 seconds later. No GPS data was found reference this event.
H46R9T	According to the finding from suspect's phone we found that 1.The phone's owner (Steven Lefft). 2. Mr. Steven lefft contact Mr. Harris Marvins via e-mail about "Inheritance". 3. Phone number of Mr. Harris Marvins is recorded to this phone. Summary Result: According to the evidence we can

TABLE 2

WebCode	Additional Comments
	indentify that Mr. Steven lefft might be implicate in this crime and he was working with "Paul" due to Paul had sent next scam namely "George Trews " to Steve.
JVM7CV	Software used: UFED Physical Analyzer V 4.2.1.7 Oxigen Forensics 7.3.0.435
LHAK2Z	The proficiency test was much better than last year's beta. However, I find it unusual that the physical was extracted using Mobile Phone Examiner Plus. I realize that this has no bearing on the test, but it's certainly not a common examiners tool. Maybe in the future, the tool that was used doesn't need to be mentioned.
RY2BNW	May of the questions were very vague. When dealing with the viber app there were multiple databases and to narrow down the actual last opened date. There were also multiple searches in google maps. I was unsure as to what you wanted. Did you want the first search the actualy search that resulted in directions.
RYWRZT	Could not answer questions 5, 6 appropriately or 11 & 13. We do not have software "AccessData MPE", assuming that that program is able to parse the data that you're looking for in those particular questions(clipboard, bluetooth connections made & "city last turned on" is not a function supported by our tools. In addition, dates of 12/12/2014 in the GPS were missing even though the last date powered on showed 12/12/2014 in the power logs using Cellebrite P.A.). I did my best using Cellebrite P.A. and Oxygen. Also, my screen on this page says "Page 7 of 8" I don't see any of tabs available to access a supposed Page 8. Only options that I have are save and save and close.
UCCT9V	6. According to the SYSTEM_BOOT@ calls found in the physical dump corresponding to boot times of the phone, the mobile telephone was last started at 12-12-2014 9:15:02(UTC-5) and shutdown (according to poweroff_log.txt) 6 seconds later at 12-12-2014 9:15:08(UTC-5). It appears the mobile telephone was never fully booted to the point where the PREVIOUS_SYS_TIME setting in the settings.db (android providers' settings) was updated. We have therefore considered this boot to have been an accidental and partial boot and have ignored it in the answering of this question. 12. According to the Samsung logs (/data/data/com.samsung.android.providers.context/databases/ContextDB.db) the app was started at 11-12-2014 08:24:45 GMT-5, however the Viber database (/data/data/com.viber.voip/databases/viber_messages > adx table) states that the app was launched 7 seconds later. 15. Exif data, in itself, does not "display" (verb). Applications, however, *do* display (verb). The representation of the binary format of the metadata is dependent on the application used to display the metadata and the precision thereof. 21. This is according to our definition of "search using google", which we take as meaning a 'web search using google.com'. However, strictly speaking, "search using Google" should also incorporate the search in Google PlayStore and therefore also the answers of question 14.
UD8CCH	Examination of extracted data partition indicates that Mr. Lefft was involved in the crime of Identity Theft. There are multiple emails in the mobile phone that can prove that. He was working with another person named Mr. Paul (Paul Gee). This can be proved with the help of conversations between Mr. Lefft and Mr. Paul. Conversation between Mr. Lefft and Mr. Paul also indicates that Mr. Left applied for loan in a bank. It is also revealed during the examination that Mr. Paul and Mr. Lefft had a discussion about their next target for their scam who is identified to be George Trews. During the investigation of this case two deleted Facebook chats and one deleted skype chats were found between 3rd June 2014 to 5th June 2014. In these chats a plan is made to grab someone who goes to 'potowmack elementary school'. The Participants of the Facebook chat were (100004303518291) Jordan Mikes, (100004703264827) Pete Aye and (100008364526130) Chet McStevens. Two locations associated with Facebook chats were also identified as (39.025366, -77.406347) and (39.025191, -77.406508). The participant of the skype chats were pcot21331 (pcot21331) and likejordan21331 (Jordan m). This could be a

TABLE 2

WebCode	Additional Comments
	possible lead into some missing person case. Some facebook profiles were opened from this phone. May any person among these facebook profiles would be the target or have any relations with Mr. Lefft.
ULK4ZV	Different applications present the EXIF data differently. This poses a problem for question number 15.
ZYQ8TH	Based on the evidence presented Suspect-Lefft was in communication with a another confederate by the name of Paul. It appears both Lefft and Paul were already planning on de-frauding another individual by the name of George Trews. After several searches I was not able to locate a google map search. I used a grep search for https://www.google.com/maps/dir/ with no result.