Collaborative Testing Services, Inc
FORENSIC TESTING PROGRAM

Mobile Digital Evidence
Test No. 16-5550 Summary Report

This proficiency test was sent to 88 participants. Participants were provided with data yielded from a physical extraction of a smart phone. They were asked to analyze the sample and answer scenario based questions utilizing their own tools and methods. Data was returned from 80 participants (91% response rate) and are compiled in the following tables:

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 sections, and will change with every report.

Printed: October 24, 2016

Manufacturer's Information

The Mobile Digital examination test consisted of data extracted from a smartphone. The sample data was provided in .dd and .bin formats. Participants were asked to examine the provided data utilizing their own tools and methods.

SAMPLE PREPARATION:

The phone data was generated following a scripted scenario based upon a toilet-papering (pseudo bomb threat). The script was planned and executed in early February 2016. A LG Leon MS345 smartphone was used to perform the scripted activities to generate the intended digital artifacts.

The phone data was obtained through a physical extraction of the LG Leon MS345 smartphone utilizing Cellebrite's UFED Physical Analyzer. Following sample validation the phone data was stored into .dd and .bin archives and compressed. MD5 and SHA-1 algorithms were run on the compressed files to generate unique hash values to allow participants to validate the successful download of the compressed files. The data archives were uploaded to the CTS portal for participants to download.

SAMPLE VALIDATION/VERIFICATION:

The validation stage consisted of the examination of the phone data utilizing various tools and methods to ensure expected results could be achieved. Laboratories that conducted predistribution analysis of the sample data reported consistent results.

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

SCENARIO PROVIDED TO PARTICIPANTS

NOTE: In the scenario below the act of toilet-papering the school has been substituted for the act of bombing the school. Therefore, whenever a reference to toilet papering the school is made, the examiner is to evaluate it as a serious offense such as a bomb threat against the school.

Scenario: On February 4, 2016, Keys High School received toilet-papering threats against Keys High School. Local police were canvassing the school premises when they discovered an abandoned LG Leon MS345 smartphone in the women's locker room. Police took the phone into evidence and created a physical image. You have been tasked with analyzing the image of the phone and identifying any owner information and/or information that links the phone with any of the threats made against the school.

Manufacturer's Information, continued

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

1 Provide the MD5 hash value for the provided image file.

e40d2ea0dfc645c9306c5edde32a47c6

2 Provide the SHA1 (base 16) hash value for the provided image file.

b8eb790235659224f6119188851de6c1827d1c6b

3** What is the device name as reported in the android provider's settings?

LGE LGMS345

4 According to the calendar, what time zone is this device configured to? (ANSWER MUST BE PRESENTED AS "Country/City")

America/New_York

5 As per the LGE weather settings, which city/state is set as the location? (ANSWER MUST BE PRESENTED AS "City, State")

Dulles Town Center, Virginia

6 To what wireless network(s) has this device been connected?

Google Starbucks

7 Do the connected wireless network(s) require a psk (password), if so what are they?

No

8 What is the name of the Bluetooth device that this device was connected to?

KIA Motors

9** What date was the Bluetooth connection made? (ANSWER MUST BE PRESENTED AS DD-Month-YYYY; HH:MM:SS –UTC)

04-February-2016; 14:18:57 UTC

10 How many calendar events are associated with this device?

Four (4)

11 What are the memos(names) of the Alarms set on this device?

Wake-up
Revenge

12 List the first third-party application to be downloaded onto the device. (ANSWERS MUST HAVE BOTH THE "package_name" and "title")

Package_name: "Com.tumblr"
Title: "Tumblr"

13 What term(s) were searched for in the Google Play Store?

tumblr

Manufacturer's Information, continued

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

14 What is the blog name for the Tumblr account associated with this device?

torturedteenagesoul88

15 What is the title and content of the body for the first Tumblr post created by a user with this device?

Title: "Thoughts"
Contents of Body: "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…"

16 What is the identifier name of the external user that communicates with the active Tumblr account on this device?

lazystranger63

17 What is lazystranger63's google hangout account username? (Provide full username as it is presented in the comment)

blackserpent34@gmail.com

18 In Google maps a user requested driving directions to a park. Provide the full name of the park.

Algonkian Regional Park

19 What terms did the suspect search for via Google search engine? (items only need to be listed once)

TP-ing
Best Toilet Paper
Charmin Ultra Soft

20 What are the names of the downloaded items via Google Chrome?

download.jpg
download(1).jpg

21 Via Instagram a picture of a suspension slip was posted. What is the student ID # on the slip?

190199

22 What is the name of the attachment that is sent via google hangouts?

DIY_Toilet%2BPaper.PNG

23 Which third-party application was the last to be downloaded on Friday, January 22, 2016? (ANSWERS MUST HAVE BOTH THE "package_name" and "title")

Package_name: "com.facebook.orca"
Title: "Messenger"

24 What is the body of the first message received via Skype from user Diane Chambers?

Heard you failed the test! Serves you right dumb girl.

25 Please list the display name associated for the following contact number- 7039402942

Lisa Frank

Manufacturer's Information, continued

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

26 What phone number is associated with the following user names: LazyStranger63, blackserpent34, and LazyStranger45?

571-645-9269

27** When does the first call with Lisa Frank start via Skype? (ANSWER MUST BE PRESENTED AS: DD-Month-YYYY; HH:MM:SS- UTC)

01 February 2016 13:49:15 UTC

28 What is the phone number for Keys High School?

571-434-1925

29 How many times was Keys High School called?

Four (4)

30 Did Mr. Black call this device on the day it was found by police, February 4, 2016?

Yes

31** How many voicemails were left on this device by contact Lisa Frank?

Two (2)

32 What does Blackserpent34 suggest that TourturedTeenageSoul88 do to their school?

T-P the school

33 What is the name of the attachment Diane Chambers sends in a group e-mail?

Falling_Stella.jpg

34 What is the google e-mail address associated with this device? (ANSWER MUST BE PROVIDED AS FULL ADDRESS)

st3llar8@gmail.com

35 What is the Yahoo e-mail address associated with this device?

notyouraveragejoe78@yahoo.com

36** How many e-mails were sent using the Yahoo account?

Three (3)

37 From your analysis what is the name associated with the primary accounts on this device?

Stella Frost

38 From your analysis was this device used to plan for the toilet papering of Keys High School?

Yes

39 From your analysis was this device used to make the threat to Keys High School?

Yes

Manufacturer's Information, continued

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

40** Was a list of targets found? If so, what names were on the list? (Provide real names)

Yes
Lisa
Hilary
Diane
Principal Skinner
Ms. Krabappel

41** At the conclusion of your analysis of the device are there any persons of interest? (Provide real names)

Yes
Stella Frost
Lex Luther

Summary Comments

The 16-5550 Mobile Digital Evidence test was designed to allow participants to assess their proficiency in examining digital artifacts obtained from a smart phone utilizing their own tools and methods. Data from a physical extraction of a smart phone along with a scripted scenario was provided to participants. (See Manufacturer's Information for preparation details, test scenario, and test questions.)

Participants were requested to analyze digital artifacts addressing common examination areas such as: image details, phone & network settings, applications, communications, and analysis.

Consensus was achieved for a majority of the questions asked. However, seven questions did not achieve a consensus (3, 9, 27, 31, 36, 40, and 41). Question 3 dealt with the device name as provided in the Android provider's settings. Question 9 and 27 dealt with time and conversion issues. Question 31 dealt with the number of voicemail messages. Question 36 dealt with the number of e-mails sent from a specific account. Question 40 dealt with a list of targets. Question 41 dealt with persons of interest.

Within the analysis category of questions (38, 39, 40, & 41) some participants reported that this type of analysis was beyond their scope of work. These questions were designed to challenge the participants' ability to summarize, analyze, and infer the answers subject to the entire data set from the proposed scenario.

CTS acknowledges that the Scenario released with the Test on May 12, 2016 contained the incorrect date of the toilet-papering threats (January 21, 2016). This was updated on June 9, 2016 to the correct date of February 4, 2016. Participants were notified of the error at the time of this change. This did not appear to affect any participant's responses.

Based on the additional comments received from the participants, specific sections will be addressed and improved in future tests, with a focus on question specificity and data format parameters. This will help increase the consistency of establishing consensus from the participants' responses.

Digital Evidence Responses

TABLE 1

Question 1 - Image Details

Question 1: Provide the MD5 hash value for the provided image file.

Manufacturer's Expected Response: e40d2ea0dfc645c9306c5edde32a47c6

WebCode	Response
2EKP2R	e40d2ea0dfc645c9306c5edde32a47c6
2L4XFF	e40d2ea0dfc645c9306c5edde32a47c6
2T3MWK	e40d2ea0dfc645c9306c5edde32a47c6
2ZYCPH	e40d2ea0dfc645c9306c5edde32a47c6
3XNA9L	e40d2ea0dfc645c9306c5edde32a47c6
4EAWZL	e40d2ea0dfc645c9306c5edde32a47c6
67DGNM	Downloaded file- MD5: B9C1880B2EAFE7AD1A7A2FC3FCEEBC37 Downloaded file - Unzipped MD5:E40D2EA0DFC645C9306C5EDDE32A47C6
6B4QXK	e40d2ea0dfc645c9306c5edde32a47c6
6FZH7G	e40d2ea0dfc645c9306c5edde32a47c6
6JJAHK	E40D2EA0DFC645C9306C5EDDE32A47C6
6KETJL	e40d2ea0dfc645c9306c5edde32a47c6
76HXLK	e40d2ea0dfc645c9306c5edde32a47c6
77PFKG	e40d2ea0dfc645c9306c5edde32a47c6
7BNU7K	E40D2EA0DFC645C9306C5EDDE32A47C6
7K8NDH	E40D2EA0DFC645C9306C5EDDE32A47C6
8BHWAF	E40D2EA0DFC645C9306C5EDDE32A47C6
8DP7RD	bin- e40d2ea0dfc645c9306c5edde32a47c6
9AEBRE	e40d2ea0dfc645c9306c5edde32a47c6
9CPE9B	C1860CBC53409012D5E8140AF51ED8B
A2MFXG	e40d2ea0dfc645c9306c5edde32a47c6
AWRL2F	e40d2ea0dfc645c9306c5edde32a47c6
AZRXWF	E40D2EA0DFC645C9306C5EDDE32A47C6
B4BFFC	MD5: e40d2ea0dfc645c9306c5edde32a47c6 (FTK Imager Version 3.4.2.6)
BX4PD7	The following hash value was obtained by hashing the zip file as a single file in EnCase: e40d2ea0dfc645c9306c5edde32a47c6
C3CNWB	E40D2EA0DFC645C9306C5EDDE32A47C6
C9GBYC	Both the unzipped .bin and .dd files have an MD5 hash value of: e40d2ea0dfc645c9306c5edde32a47c6
D37Q26	E40D2EA0DFC645C9306C5EDDE32A47C6
D8L2EA	E40D2EA0DFC645C9306C5EDDE32A47C6
DHJ3QD	b9c1880b2eafe7ad1a7a2fc3fceebc37
DJFH4A	e40d2ea0dfc645c9306c5edde32a47c6
DRKPJA	D41D8CD98F00B204E9800998ECF8427E

TABLE 1

Question 1 - Image Details

WebCode	Response
E3HPVE	b9c1880b2eafe7ad1a7a2fc3fceebc37
EG36YD	E40D2EA0DFC645C9306C5EDDE32A47C6
EMVHN9	e40d2ea0dfc645c9306c5edde32a47c6
FWP664	E40D2EA0DFC645C9306C5EDDE32A47C6
FXKN86	E40D2EA0DFC645C9306C5EDDE32A47C6
G63GVA	e40d2ea0dfc645c9306c5edde32a47c6
GKUDX6	e40d2ea0dfc645c9306c5edde32a47c6
GNTPT6	E40D2EA0DFC645C9306C5EDDE32A47C6
GQNYD8	e40d2ea0dfc645c9306c5edde32a47c6 (16-5550 Image Data_BIN File.bin)
GRQTE7	b9c1880b2eafe7ad1a7a2fc3fceebc37
JZ4RHZ	e40d2ea0dfc645c9306c5edde32a47c6
K7GAZZ	E40D2EA0DFC645C9306C5EDDE32A47C6
KGL8Y2	B9C1880B2EAFE7AD1A7A2FC3FCEEBC37
KJ6YQY	e40d2ea0dfc645c9306c5edde32a47c6
KJNZ38	E40D2EA0DFC645C9306C5EDDE32A47C6
KNHWRY	e40d2ea0dfc645c9306c5edde32a47c6
KUA4A8	The raw forensic image file (16-5550 Image Data_DD File) was added as evidence into Forensic ToolKit - Imager (FTK Imager). FTK Imager was utilized to create a disk image, therefore the raw forensic image file was converted to an .E01 file (EnCase proprietary image file) and the following MD5 hash value was generated: MD5 checksum: e40d2ea0dfc645c9306c5edde32a47c6 A verification MD5 hash value was also generated, therefore verifying that the .E01 forensic image file is exactly the same as the original raw forensic image file.
KZFX43	e40d2ea0dfc645c9306c5edde32a47c6
L66WV3	e40d2ea0dfc645c9306c5edde32a47c6 - image bin file 16-5550 Image Data_BIN File.zip MD5 hash value: b9c1880b2eafe7ad1a7a2fc3fceebc37
L6LTN3	H:\H:\\16-5550%20Image%20Data_BIN%20File.zip: b9c1880b2eafe7ad1a7a2fc3fceebc37 H:\H:\\16-5550%20Image%20Data_DD%20File.zip: 6f5b9b6abdade182158800ce962f28ad
LYLK83	E40D2EA0DFC645C9306C5EDDE32A47C6
M3ZEMY	e40d2ea0dfc645c9306c5edde32a47c6
M9L8YY	e40d2ea0dfc645c9306c5edde32a47c6
MDGY8V	e40d2ea0dfc645c9306c5edde32a47c6
MHCT6X	E40D2EA0DFC645C9306C5EDDE32A47C6
NDV89V	e40d2ea0dfc645c9306c5edde32a47c6
NGBFWV	e40d2ea0dfc645c9306c5edde32a47c6
NUDXH3	MD5 hash value: b9c1880b2eafe7ad1a7a2fc3fceebc37
PK8DUZ	e40d2ea0dfc645c9306c5edde32a47c6
QCCWH2	e40d2ea0dfc645c9306c5edde32a47c6
QQ8CHV	e40d2ea0dfc645c9306c5edde32a47c6
QVK6NT	e40d2ea0dfc645c9306c5edde32a47c6
RGCV7W	E40D2EA0DFC645C9306C5EDDE32A47C6

TABLE 1

Question 1 - Image Details

WebCode	Response
RR6VHG	E40D2EA0DFC645C9306C5EDDE32A47C6
T8QRYW	e40d2ea0dfc645c9306c5edde32a47c6
TT8FBU	16-5550 Image Data_BIN File: e40d2ea0dfc645c9306c5edde32a47c6
UFLZ8U	e40d2ea0dfc645c9306c5edde32a47c6
UQC6QQ	e40d2ea0dfc645c9306c5edde32a47c6
URBWAT	e40d2ea0dfc645c9306c5edde32a47c6
V2AL8P	16-5550 Image Data_DD File.dd MD5 hash value: e40d2ea0dfc645c9306c5edde32a47c6
VHGMPN	E40D2EA0DFC645C9306C5EDDE32A47C6
VJC6QP	E40D2EA0DFC645C9306C5EDDE32A47C6
VN3F2M	E40D2EA0DFC645C9306C5EDDE32A47C6
WWD2MW	e40d2ea0dfc645c9306c5edde32a47c6
XN3Y2V	e40d2ea0dfc645c9306c5edde32a47c6
YHLTAN	E40D2EA0DFC645C9306C5EDDE32A47C6
ZKATLG	e40d2ea0dfc645c9306c5edde32a47c6
ZVTJVL	E40D2EA0DFC645C9306C5EDDE32A47C6
ZWTAEN	.bin file: e40d2ea0dfc645c9306c5edde32a47c6

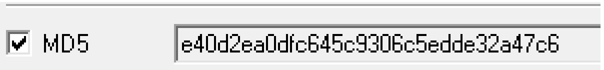
Consensus Result: e40d2ea0dfc645c9306c5edde32a47c6

Expected Response Explanation:

This hash value can be achieved by decompressing the supplied .zip file and running a MD5 hash algorithm on the image file.

Expected Response Illustration:

MD5 Hash Value:



☑ MD5 e40d2ea0dfc645c9306c5edde32a47c6

Other Responses:

Six participants appear to have reported the MD5 hash value for the compressed 16-5550 Image Data_BIN File.zip (B9C1880B2EAFE7AD1A7A2FC3FCEEBC37). This was provided with the data download to assist with confirmation of a successful download prior to decompressing and performing any examination.

TABLE 1

Question 2 - Image Details

Question 2: Provide the SHA1 (base 16) hash value for the provided image file.

Manufacturer's Expected Response: b8eb790235659224f6119188851de6c1827d1c6b

WebCode	Response
2EKP2R	b8eb790235659224f6119188851de6c1827d1c6b
2L4XFF	b8eb790235659224f6119188851de6c1827d1c6b
2T3MWK	b8eb790235659224f6119188851de6c1827d1c6b
2ZYCPH	b8eb790235659224f6119188851de6c1827d1c6b
3XNA9L	b8eb790235659224f6119188851de6c1827d1c6
4EAWZL	b8eb790235659224f6119188851de6c1827d1c6b
67DGNM	Downloaded file-SHA1: 3C800982B399E38943F7F006F177651C96F847A7 Downloaded file Unzipped - SHA1:B8EB790235659224F6119188851DE6C1827D1C6B
6B4QXK	b8eb790235659224f6119188851de6c1827d1c6b
6FZH7G	b8eb790235659224f6119188851de6c1827d1c6b
6JJAHK	B8EB790235659224F6119188851DE6C1827D1C6B
6KETJL	b8eb790235659224f6119188851de6c1827d1c6b
76HXLK	b8eb790235659224f6119188851de6c1827d1c6b
77PFKG	b8eb790235659224f6119188851de6c1827d1c6b
7BNU7K	B8EB790235659224F6119188851DE6C1827D1C6B
7K8NDH	B8EB790235659224F6119188851DE6C1827D1C6B
8BHWAF	B8EB790235659224F6119188851DE6C1827D1C6B
8DP7RD	bin- b8eb790235659224f6119188851de6c1827d1c6b
9AEBRE	B8EB790235659224F6119188851DE6C1827D1C6B
9CPE9B	F75259B5ABF180A68C357768671BBF7C8CD8BF27
A2MFXG	b8eb790235659224f6119188851de6c1827d1c6b
AWRL2F	b8eb790235659224f6119188851de6c1827d1c6b
AZRXWF	B8EB790235659224F6119188851DE6C1827D1C6B
B4BFFC	SHA1: b8eb790235659224f6119188851de6c1827d1c6b (FTK Imager Version 3.4.2.6)
BX4PD7	The following hash value was obtained by hashing the zip file as a single file in EnCase: B8EB790235659224F6119188851DE6C1827D1C6B The next hash value was obtained in UFED Physical Analyzer under the Legacy tab. This is the hash value that was calculated for the extraction within UFED Physical Analyzer: SHA256 F9BC803862BE0EFC1F0C9ABC15AF5D96FE64DF7E9F4C6C303E16A783587DAA2A
C3CNWB	B8EB790235659224F6119188851DE6C1827D1C6B
C9GBYC	Both the unzipped .bin and .dd files have a SHA1 hash value of: b8eb790235659224f6119188851de6c1827d1c6b
D37Q26	B8EB790235659224F6119188851DE6C1827D1C6B
D8L2EA	B8EB790235659224F6119188851DE6C1827D1C6B
DHJ3QD	3c800982b399e38943f7f006f177651c96f847a7
DJFH4A	b8eb790235659224f6119188851de6c1827d1c6b
DRKPJA	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

TABLE 1

Question 2 - Image Details

WebCode	Response
E3HPVE	3c800982b399e38943f7f006f177651c96f847a7
EG36YD	B8EB790235659224F6119188851DE6C1827D1C6B
EMVHN9	b8eb790235659224f6119188851de6c1827d1c6b
FWP664	B8EB790235659224F6119188851DE6C1827D1C6B
FXKN86	B8EB790235659224F6119188851DE6C1827D1C6B
G63GVA	b8eb790235659224f6119188851de6c1827d1c6b
GKUDX6	b8eb790235659224f6119188851de6c1827d1c6b
GNTPT6	B8EB790235659224F6119188851DE6C1827D1C6B
GQNYD8	b8eb790235659224f6119188851de6c1827d1c6b (16-5550 Image Data_BIN File.bin)
GRQTE7	3c800982b399e38943f7f006f177651c96f847a7
JZ4RHZ	b8eb790235659224f6119188851de6c1827d1c6b
K7GAZZ	B8EB790235659224F6119188851DE6C1827D1C6B
KGL8Y2	3C800982B399E38943F7F006F177651C96F847A7
KJ6YQY	b8eb790235659224f6119188851de6c1827d1c6b
KJNZ38	B8EB790235659224F6119188851DE6C1827D1C6B
KNHWRY	b8eb790235659224f6119188851de6c1827d1c6b
KUA4A8	The raw forensic image file (16-5550 Image Data_DD File) was added as evidence into Forensic ToolKit - Imager (FTK Imager). FTK Imager was utilized to create a disk image, therefore the raw forensic image file was converted to an .E01 file (EnCase proprietary image file) and the following SHA1 hash value was generated: SHA1 checksum: b8eb790235659224f6119188851de6c1827d1c6b A verification SHA1 hash value was also generated, therefore verifying that the .E01 forensic image file is exactly the same as the original raw forensic image file.
KZFX43	b8eb790235659224f6119188851de6c1827d1c6b
L66WV3	b8eb790235659224f6119188851de6c1827d1c6b image bin file 16-5550 Image Data_BIN File.zip SHA1 hash value: 3c800982b399e38943f7f006f177651c96f847a7
L6LTN3	H:\H:\\16-5550%20Image%20Data_BIN%20File.zip: 3c800982b399e38943f7f006f177651c96f847a7 H:\H:\ \16-5550%20Image%20Data_DD%20File.zip: d7e326cad7227363065372052cd0080c4dca1caf
LYLK83	B8EB790235659224F6119188851DE6C1827D1C6B
M3ZEMY	b8eb790235659224f6119188851de6c1827d1c6b
M9L8YY	b8eb790235659224f6119188851de6c1827d1c6b
MDGY8V	b8eb790235659224f6119188851de6c1827d1c6b
MHCT6X	B8EB790235659224F6119188851DE6C1827D1C6B
NDV89V	b8eb790235659224f6119188851de6c1827d1c6b
NGBFWV	b8eb790235659224f6119188851de6c1827d1c6b
NUDXH3	SHA1 hash value: 3c800982b399e38943f7f006f177651c96f847a7
PK8DUZ	b8eb790235659224f6119188851de6c1827d1c6b
QCCWH2	b8eb790235659224f6119188851de6c1827d1c6b
QQ8CHV	b8eb790235659224f6119188851de6c1827d1c6b

TABLE 1

Question 2 - Image Details

WebCode	Response
QVK6NT	b8eb790235659224f6119188851de6c1827d1c6b
RGCV7W	B8EB790235659224F6119188851DE6C1827D1C6B
RR6VHG	B8EB790235659224F6119188851DE6C1827D1C6B
T8QRYW	b8eb790235659224f6119188851de6c1827d1c6b
TT8FBU	16-5550 Image Data_BIN File: b8eb790235659224f6119188851de6c1827d1c6b
UFLZ8U	b8eb790235659224f6119188851de6c1827d1c6b
UQC6QQ	b8eb790235659224f6119188851de6c1827d1c6b
URBWAT	b8eb790235659224f6119188851de6c1827d1c6b
V2AL8P	16-5550 Image Data_DD File.dd SHA1 hash value: b8eb790235659224f6119188851de6c1827d1c6b
VHGMPN	B8EB790235659224F6119188851DE6C1827D1C6B
VJC6QP	B8EB790235659224F6119188851DE6C1827D1C6B
VN3F2M	b8eb790235659224f6119188851de6c1827d1c6b
WWD2MW	b8eb790235659224f6119188851de6c1827d1c6b
XN3Y2V	b8eb790235659224f6119188851de6c1827d1c6b
YHLTAN	B8EB790235659224F6119188851DE6C1827D1C6B
ZKATLG	b8eb790235659224f6119188851de6c1827d1c6b
ZVTJVL	B8EB790235659224F6119188851DE6C1827D1C6B
ZWTAEN	.bin file: b8eb79023565922456119188851de6c1827d1c6b

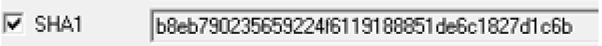
Consensus Result: b8eb790235659224f6119188851de6c1827d1c6b

Expected Response Explanation:

This hash value can be achieved by decompressing the supplied .zip file and running a SHA1 hash algorithm on the image file.

Expected Response Illustration:

SHA1 Hash Value:



☑ SHA1 b8eb790235659224f6119188851de6c1827d1c6b

Other Responses:

Five participants appear to have reported the SHA1 hash value for the compressed 16-5550 Image Data_BIN File.zip (3C800982B399E38943f7F006F177651C96f847A7). This was provided with the data download to assist with confirmation of a successful download prior to decompressing and performing any examination.

TABLE 1

Question 3 - Phone & Network Settings

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

Manufacturer's Expected Response: LGE LGMS345

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
2EKP2R	the Android ID is 37C101f07d4862d8
2L4XFF	FROSTY
2T3MWK	LGMS345
2ZYCPH	LG Leon LTE
3XNA9L	LGMS345 ? FROSTY
4EAWZL	LGE LGMS345
67DGNM	FROSTY Location:ImageData_BINFile.bin/userdata/data/com.android.providers.settings/databases/settings.db
6B4QXK	FROSTY
6FZH7G	FROSTY
6JJAHK	FROSTY
6KETJL	FROSTY LGE LGMS345 LG Leon LTE
76HXLK	FROSTY
77PFKG	FROSTY
7BNU7K	FROSTY
7K8NDH	LGE LGMS345
8BHWAF	LGE LGMS345
8DP7RD	FROSTY
9AEBRE	LGMS345
9CPE9B	LGMS345
A2MFXG	LG Leon LTE, LGE LGMS345, FROSTY
AWRL2F	LGMS345
AZRXWF	com.android.provider.settings /databases/settings.db 420= lg_device_name Value = FROSTY
B4BFFC	FROSTY. (settings.db, System table)
BX4PD7	The LG_device_name is LG Leon LTE and the model which is listed in the file system folder as device_name is LGE LGMS345.
C3CNWB	c50_mpcs_us
C9GBYC	FROSTY
D37Q26	LGE LGMS345
D8L2EA	FROSTY
DHJ3QD	LGE LGMS345
DJFH4A	FROSTY
DRKPJA	Owner
E3HPVE	LGE LGMS345
EG36YD	FROSTY
EMVHN9	Under the android provider's settings, the device name is "FROSTY" without the quotations.

TABLE 1

Question 3 - Phone & Network Settings

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
FWP664	LGE LGMS345
FXKN86	Stella Frost
G63GVA	In the com.android.providers.settings, in the settings.db in global the device name is listed twice LG Leon LTE and LGE LGMS345. In the same db in system the lg_device_name is FROSTY.
GKUDX6	LGE LGMS345 userdata (ExtX)/Root/data/com.android.providers.settings/databases/settings.db
GNTPT6	LGE LGMS345
GQNYD8	FROSTY
GRQTE7	LGE LGMS345 / LG Leon LTE
JZ4RHZ	FROSTY
K7GAZZ	LGE LGMS345
KGL8Y2	FROSTY
KJ6YQY	Device name is: LGE LGMS345
KJNZ38	FROSTY
KNHWRY	LGE LGMS345
KUA4A8	I navigated to the android provider's settings directory (data/com.android.providers.settings), where I viewed all of the content within this folder. The settings database file (settings.db) was located inside of the database folder (data/com.android.providers.settings/database/settings.db), exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, the device name is as follows: - LG_DEVICE_NAME = LG Leon LTE - DEVICE_NAME = LGE LGMS345
KZFX43	LGE LGMS345
L66WV3	FROSTY LGE LGMS345
L6LTN3	FROSTY (settings.db --> System --> lg_device_name) LG Leon LTE (settings.db --> Global --> lg_device_name) LGE LGMS345 (settings.db --> Global --> device_name)
LYLK83	LG Leon LTE or LGE LGMS345
M3ZEMY	There were three device names located in the android provider settings database file, they are listed as follows: Device Name=LGE LGMS345 LG Device Name= LG Leon LTE LG Device Name= FROSTY
M9L8YY	FROSTY
MDGY8V	LGE LGMS345
MHCT6X	LG LEON LTE LGE LGMS345
NDV89V	LGE LGMS345
NGBFWV	LGE LGMS345
NUDXH3	LG Leon LTE
PK8DUZ	FROSTY
QCCWH2	LG_MS345
QQ8CHV	Owner
QVK6NT	LGE LGMS345
RGCV7W	FROSTY
RR6VHG	1- LG LEON LTE 2- LGMS345

TABLE 1

Question 3 - Phone & Network Settings

** No consensus achieved; Inconsistencies not highlighted **

WebCode	Response
T8QRYW	Provider’s database settings file, record 89 lists “device_name” = LGE LGMS345 Also identified another record within the provider’s database settings file, record 5 lists “LG_device_name” = LG Leon LTE
TT8FBU	FROSTY
UFLZ8U	c50_mpcs_us A Bluetooth device name of 'Frosty' was also recovered.
UQC6QQ	FROSTY
URBWAT	LGE LGMS345 (device_name) LG Leon LTE (lg_device_name) Frosty (LG_device_name)
V2AL8P	LGE LGMS345
VHGMPN	LGE LGMS345
VJC6QP	LGE LGMS345
VN3F2M	LGE LGMS345
WWD2MW	LGE MS345
XN3Y2V	LGMS345 User named device FROSTY.
YHLTAN	LGE LGMS345
ZKATLG	Frosty device ID: 37c101f07d4862d8
ZVTJVL	Stella Frost
ZWTAEN	Frosty

TABLE 1

Question 3 - Phone & Network Settings

Consensus Result: ** No consensus achieved; Inconsistencies not highlighted **

Expected Response Explanation:

Consensus was not achieved for question 3. Variations of responses are due to multiple device names listed on this device within the settings database:

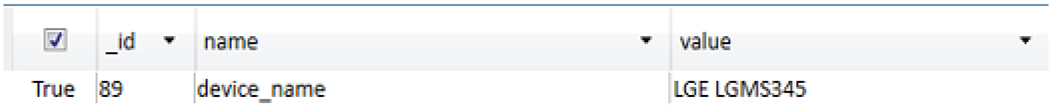
Device names found within the global table at:
\data\com.android.providers.settings\databases\settings.db.
LGE LGMS 345 - 44 participants
LG Leon LTE - 13 participants

Device names found within the system table at:
\data\com.android.providers.settings\databases\settings.db.
FROSTY - 37 participants

The total number of participants listed above is greater than the number of participants due to participants reporting multiple device names.

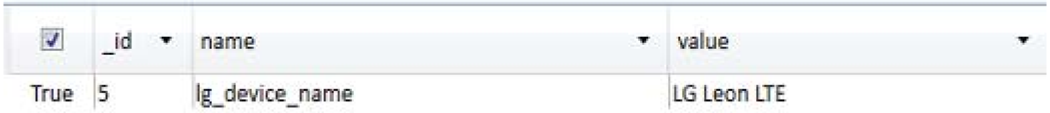
Expected Response Illustration:

Database: settings >>>Table: global



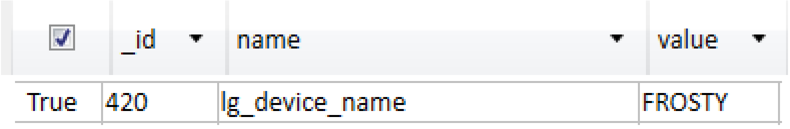
☑	_id	name	value
True	89	device_name	LGE LGMS345

Database: settings >>> Table: global



☑	_id	name	value
True	5	lg_device_name	LG Leon LTE

Database: settings >>> Table: system



☑	_id	name	value
True	420	lg_device_name	FROSTY

TABLE 1

Question 4 - Phone & Network Settings

Question 4: According to the calendar, what time zone is this device configured to? (ANSWER MUST BE PRESENTED AS "Country/City")

Manufacturer's Expected Response: America/New_York

WebCode	Response
2EKP2R	America/New York
2L4XFF	America/New_York
2T3MWK	USA/New York
2ZYCPH	America/New_York
3XNA9L	America/New_York
4EAWZL	America/New_York
67DGNM	America/New York Location:ImageData_BINFile.bin/userdata/data/com.android.providers.calendar/databases/calendar.db
6B4QXK	America/New_York
6FZH7G	America/New York
6JJAHK	America/New_York
6KETJL	America/New_York
76HXLK	America/New_York
77PFKG	America/New York
7BNU7K	America/New York
7K8NDH	America/New_York
8BHWAF	America/New_York
8DP7RD	America/New York
9AEBRE	America/New York
9CPE9B	America/New York
A2MFXG	America/New_York
AWRL2F	America/New York
AZRXWF	America/New York
B4BFFC	America/New York. (Cellebrite Extraction Report - Device Information)
BX4PD7	America/New_York
C3CNWB	America/New_York
C9GBYC	America/New_York
D37Q26	America/New York
D8L2EA	America/New York
DHJ3QD	America/New York
DJFH4A	America/New York
DRKPJA	America/New York
E3HPVE	America/New York
EG36YD	America/New_York

TABLE 1

Question 4 - Phone & Network Settings

WebCode	Response
EMVHN9	America/New_York
FWP664	America/New_York
FXKN86	America/New_York
G63GVA	America/New York
GKUDX6	America/New_York userdata (ExtX)/Root/data/com.android.calendar/shared_prefs/com.android.calendar_preferences.xml
GNTPT6	America/New_York
GQNYD8	America/New_York
GRQTE7	America/New York
JZ4RHZ	America/New_York
K7GAZZ	America/New_York
KGL8Y2	America/New_York
KJ6YQY	America/New York
KJNZ38	America/New York
KNHWRY	"America/New_York"
KUA4A8	I navigated to the calendar directory (data/com.android.calendar), where I viewed all of the content within this folder. The calendar preferences file (com.android.calendar_preference.xml) was located inside of the cache folder (data/com.android.calendar/cache) and viewed as a document file within the EnCase 7 application, where the device time zone information was configured to: - AMERICA/NEW_YORK
KZFX43	America/New York
L66WV3	America/New_York
L6LTN3	America/New York
LYLK83	America/New York
M3ZEMY	America/New York
M9L8YY	America/New_York
MDGY8V	America/New_York
MHCT6X	America/New_York
NDV89V	America/New_York
NGBFWV	America/New_York
NUDXH3	America/New York
PK8DUZ	America/New York
QCCWH2	America/New_York
QQ8CHV	America/New_York
QVK6NT	America/New_York
RGCV7W	America/New York
RR6VHG	America/New_York
T8QRYW	America/New York
TT8FBU	America/New_York

TABLE 1

Question 4 - Phone & Network Settings

WebCode	Response
UFLZ8U	America/New_York
UQC6QQ	America/New York
URBWAT	America/New York
V2AL8P	America/New_York
VHGMPN	America/New York
VJC6QP	America/New York
VN3F2M	America/New_York
WWD2MW	America/New York
XN3Y2V	America/New York
YHLTAN	America/New_York
ZKATLG	America/New York
ZVTJVL	America/New_York
ZWTAEN	America/New York

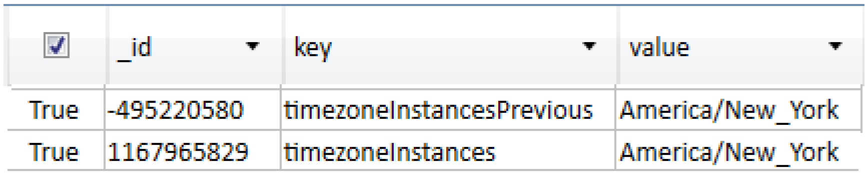
Consensus Result: America/New_York

Expected Response Explanation:

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

Expected Response Illustration:

Database: calendar >>> Table: calendar cache



☑	_id	key	value
True	-495220580	timezoneInstancesPrevious	America/New_York
True	1167965829	timezoneInstances	America/New_York

TABLE 1

Question 5 - Phone & Network Settings

Question 5: As per the LGE weather settings, which city/state is set as the location? (ANSWER MUST BE PRESENTED AS "City, State")

Manufacturer's Expected Response: Dulles Town Center, Virginia

WebCode	Response
2EKP2R	Dulles Town Center, VA
2L4XFF	Dulles Town Center, Virginia
2T3MWK	Sterling,Virginia (Dulles Town Center)
2ZYCPH	Dulles Town Center, Virginia
3XNA9L	Dulles Town Center, Virginia
4EAWZL	Dulles Town Center, Virginia
67DGNM	Dulles Town Center, Virginia Location:ImageData_BINFile.bin/userdata/data/com.lge.settings.weather.platform/databases/WEATHER_SERVICE.db
6B4QXK	Dulles Town Center, Virginia
6FZH7G	Dulles Town Center, Virginia
6JJAHK	Dulles, Virginia Wording in Settings: Dulles Town Center, Virginia
6KETJL	Dulles Town Center, Virginia
76HXLK	Dulles Town Center, Virginia
77PFKG	Dulles Town Center/Virginia
7BNU7K	Dulles Town Center, Virginia
7K8NDH	Dulles Town Center, Virginia
8BHWAF	Dulles Town Center, Virginia
8DP7RD	Dulles Town Center,VA
9AEBRE	Sterling, Virginia
9CPE9B	Dulles, Virginia
A2MFXG	Dulles Town Center, Virginia
AWRL2F	Dulles Town Center, Virginia
AZRXWF	Dulles Town Center, VA
B4BFFC	Dulles, Virginia. (WEATHER_SERVICE.db, Clweather table)
BX4PD7	Virginia, Dulles Town Center
C3CNWB	Dulles Town Center/Virginia
C9GBYC	Dulles Town Center, Virginia
D37Q26	Dulles Town Center/Virginia
D8L2EA	Dulles Town Center, Virginia
DHJ3QD	Dulles Town Center, Virginia
DJFH4A	Dulles Town Center, Virginia
DRKPJA	Dulles Town Center, VA
E3HPVE	Dulles Town Center, Virginia
EG36YD	Dulles Town Center, Virginia

TABLE 1

Question 5 - Phone & Network Settings

WebCode	Response
EMVHN9	Dulles Town Center, Virginia
FWP664	Dulles Town Center, Virginia
FXKN86	Dulles Town Center
G63GVA	Dulles Town Center, Virginia
GKUDX6	Virginia / United States userdata (ExtX)/Root/data/com.lge.sizechangable.weather.platform/databases/WEATHER_SERVICE.db
GNTPT6	Dulles Town Center / Virginia
GQNYD8	Dulles Town Center, Virginia
GRQTE7	Dulles Town Center / Virginia / United States
JZ4RHZ	Dulles Town Center, Virginia
K7GAZZ	Dulles Town Center, Virginia
KGL8Y2	Dulles Town Center, Virginia
KJ6YQY	Dulles, Virginia
KJNZ38	Dulles Town Center, Va
KNHWRY	"Dulles Town Center, Virginia"
KUA4A8	I navigated to the LGE weather settings directory (data/com.lge.sizechangable.weather), where I viewed all of the content within this folder. The current locations file (currentlocation.xml) was located inside of the cache folder (data/com.lge.sizechangable.weather/shared_prefs) and viewed as a document file within the EnCase 7 application, where the device location was set to: - DULLES TOWN CENTER, VIRGINIA
KZFX43	Dulles Town Center, Virginia
L66WV3	Dulles Town Center, Virgina
L6LTN3	Dulles Town Center, Virginia
LYLK83	Dulles Town Center, Virginia
M3ZEMY	Dulles/Virginia
M9L8YY	Dulles Town Center, Virginia
MDGY8V	Dulles Town Center, Virgina
MHCT6X	Dulles Town Center, Virginia
NDV89V	Dulles Town Center, Virginia
NGBFWV	Dulles Town Center, Virginia
NUDXH3	Dulles Town Center, Virginia
PK8DUZ	Dulles Town Center, Virgina
QCCWH2	Dulles Town Center, Virgina
QQ8CHV	Dulles, Virgina
QVK6NT	Dulles Town Center, Virginia
RGCV7W	Dulles Town Center, Virginia
RR6VHG	Dulles Town Center - Virginia
T8QRYW	Dulles Town Center, Virginia
TT8FBU	Dulles Town Center, Virginia

TABLE 1

Question 5 - Phone & Network Settings

WebCode	Response
UFLZ8U	Dulles Town Center, Virginia
UQC6QQ	Dulles Town Center, Virginia
URBWAT	Dulles, Virginia
V2AL8P	Dulles Town Center, Virginia
VHGMPN	Dulles Town Center, Virginia
VJC6QP	Dulles Town Center, Virginia
VN3F2M	Dulles Town Center, Virginia
WWD2MW	Dulles Town Center, Virginia
XN3Y2V	Dulles Town Center, VA
YHLTAN	Dulles Town Center / Virginia
ZKATLG	Could not determine. Internet history suggest Washington, DC
ZVTJVL	Dulles Town Center / Virginia
ZWTAEN	Dulles Town Center, Virginia

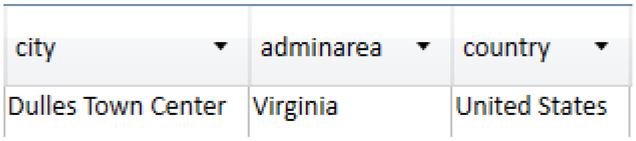
Consensus Result: Dulles Town Center, Virginia

Expected Response Explanation:

Information about the phone's weather location can be found in either the forecast_accu.db or the weather_services.db databases. These files can be found at:
data\com.lge.sizechangeable.weather\databases\forecast_accu.db
–OR-
data\com.lge.sizechangeable.weather.platform\databases\weather_services.db

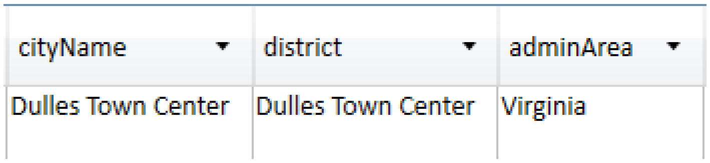
Expected Response Illustration:

Database: forecast_accu >>> Table: forecasts



city	adminarea	country
Dulles Town Center	Virginia	United States

Database: weather_services >>> Table: clweather



cityName	district	adminArea
Dulles Town Center	Dulles Town Center	Virginia

TABLE 1

Question 6 - Phone & Network Settings

Question 6: To what wireless network(s) has this device been connected?

Manufacturer's Expected Response: Google Starbucks

WebCode	Response
2EKP2R	The device appears to have connected to Google Starbucks. The other network data present on the device appears to be "test" and "example" data. The Google Starbucks network data appears to be 'real' data.
2L4XFF	Google Starbucks
2T3MWK	Google Starbucks
2ZYCPH	Google Starbucks
3XNA9L	Example, simple, Google Starbucks
4EAWZL	Google Starbucks
67DGNM	Google Starbucks Location:[ROOT]/misc/wifi/wpa_supplicant.conf
6B4QXK	"Google Starbucks"
6FZH7G	Google Starbucks
6JJAHK	Google Starbucks
6KETJL	Google Starbucks
76HXLK	Google Starbucks
77PFKG	Google Starbucks
7BNU7K	Google Starbucks
7K8NDH	Google Starbucks
8BHWAF	Google Starbucks
8DP7RD	simple,second ssid, example,1x-test,eap-fast-test,eap-sim-test,Google Starbucks,ikev2-example,leap-example,plaintext-test, static-wep-test, static-wep-test2, test adhoc.
9AEBRE	SSID: "Google Starbucks"
9CPE9B	Google Starbucks
A2MFXG	Google Starbucks
AWRL2F	Google Starbucks
AZRXWF	SSID - "Google Starbucks"
B4BFFC	Google Starbucks. (userdata(ExtX)/Root/misc/wifi/networkHistory.txt and MSAB XRY Device Extraction Report - Device/Network Information)
BX4PD7	Google Starbucks
C3CNWB	Google Starbucks
C9GBYC	Google Starbucks
D37Q26	Google Starbucks
D8L2EA	Google Starbucks The mac address of the network interface is: 40:e3:d6:69:ea:40
DHJ3QD	Google Starbucks
DJFH4A	Google Starbucks
DRKPJA	google Starbucks
E3HPVE	Google Starbucks

TABLE 1

Question 6 - Phone & Network Settings

WebCode	Response
EG36YD	Google Starbucks
EMVHN9	Google Starbucks
FWP664	Google Starbucks
FXKN86	Google Starbucks
G63GVA	Google Starbucks
GKUDX6	Google Starbucks userdata (ExtX)/Root/misc/wifi/networkHistory.txt
GNTPT6	SSID: Google Starbucks
GQNYD8	Google Starbucks
GRQTE7	Google Starbucks , example , eap-sim-test , simple , eap-psk-test , 1x-test , leap-example , ikev2-example , eap-fast-test , plaintext-test , static-wep-test , static-wep-test2 , test adhoc , second ssid
JZ4RHZ	Google Starbucks
K7GAZZ	Google Starbucks
KGL8Y2	Google Starbucks
KJ6YQY	This device was been connected to 1 Wi-Fi network. SSID of network is: Google Starbucks
KJNZ38	Google Starbucks
KNHWRY	"Google Starbucks"
KUA4A8	There are a number of ways to obtain this information, but I located a screenshot within unallocated space on the cellular device forensic image using Internet Evidence Finder (IEF). The IEF screenshot indicates that the wireless network that this device was connected to was: - GOOGLE STARBUCKS There are additional networks which show that they are available to connect this device to, but the device was not connected. These wireless networks are as follows: - CAPITALONEBANK - GO1927 - BEIGEDOVE
KZFX43	Google Starbucks
L66WV3	Google Starbucks
L6LTN3	Google Starbucks
LYLK83	Google Starbucks
M3ZEMY	Google Starbucks
M9L8YY	Google Starbucks
MDGY8V	Google Starbucks
MHCT6X	Google Starbucks
NDV89V	Google Starbucks
NGBFWV	Google Starbucks
NUDXH3	simple second ssid example leap-example ikev2-example eap-fast-test test adhoc Google Starbucks
PK8DUZ	Google Starbucks
QCCWH2	Google Starbucks
QQ8CHV	Google Starbucks
QVK6NT	Google Starbucks
RGCV7W	Google Starbucks

TABLE 1

Question 6 - Phone & Network Settings

WebCode	Response
RR6VHG	1-simple 2-second ssid 3-example 4-example 5-example 6-example 7-example 8-example 9-example 10- 11-eap-sim-test 12-eap-psk-test 13-1x-test 14-leap-example 15-ikev2-example 16-eap-fast-test 17-plaintext-test 18-static-wep-test 19-static-wep-test2 20-test adhoc 21-example 22- 23-Google Starbucks
T8QRYW	Google Starbucks
TT8FBU	1x-test,eap-fast-test,eap-psk-test,eap-sim-test,example,Google Starbucks,ikev2-example,leap-example,plaintext-test,second ssid,simple,static-wep-test,static-wep-test2,test adhoc
UFLZ8U	Google Starbucks
UQC6QQ	Google Starbucks
URBWAT	Google Starbucks
V2AL8P	Google Starbucks
VHGMPN	Google Starbucks
VJC6QP	Google Starbucks
VN3F2M	Google Starbucks
WWD2MW	simple second ssid example eap-sim-test eap-psk-test 1x-test leap-example ikev2-example eap-fast-test static-wep-test static-wep-test2 test adhoc Google Starbucks
XN3Y2V	example, eap-psk-test, leap-example, eap-fast-test, Google Starbucks
YHLTAN	Google Starbucks
ZKATLG	MetroPCS KIA Motors Google Starbucks
ZVTJVL	SSID: Google
ZWTAEN	Google Starbucks, simple, second SSID, eap-sim-test, test-adhoc, kev2-example, eap-fast-test, static-wep-test, static-wep-test2, example, eap-psk-test, 1x-test, leap-example, plaintext-test

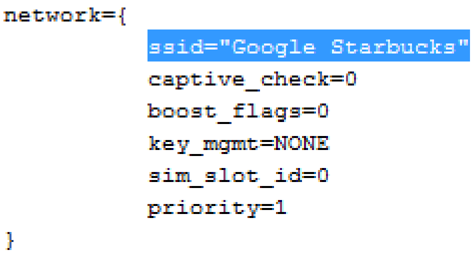
Consensus Result: Google Starbucks

Expected Response Explanation:

Information about wireless connections can be found in the wpa_supplicant.conf file. This file can be found at: data\misc\wifi\wpa_supplicant.conf

Expected Response Illustration:

Wireless Device Connection:



```
network={
          ssid="Google Starbucks"
          captive_check=0
          boost_flags=0
          key_mgmt=NONE
          sim_slot_id=0
          priority=1
}
```

TABLE 1

Question 7 - Phone & Network Settings

Question 7: Do the connected wireless network(s) require a psk (password), if so what are they?

Manufacturer's Expected Response: No

WebCode	Response
2EKP2R	The Google Starbucks wireless network has no security and does not require a password.
2L4XFF	No
2T3MWK	The connected wireless network do not require any psk.
2ZYCPH	No
3XNA9L	Not so secure passphrase, other passwords ‘foobar’, ‘password’
4EAWZL	No
67DGNM	The connected wireless networks did not require a passcode. Location: [ROOT]/misc/wifi/wpa_supplicant.conf
6B4QXK	No
6FZH7G	No
6JJAHK	No
6KETJL	None require a password
76HXLK	No
77PFKG	No
7BNU7K	No
7K8NDH	No PSK is required for any wireless networks.
8BHWAF	No
8DP7RD	(very secret passphrase, foobar), (secret passphrase),(not so secure passphrase), (foobar), (password) (very secret passphrase), (06b4be19da289f475aa46a33cb793029), (06b4be19da289f475aa46a33cb793029), (06b4be19da289f475aa46a33cb793029d4ab3db7a23ee92382eb0106c72ac7bb # priority=2)
9AEBRE	no
9CPE9B	No
A2MFXG	No
AWRL2F	No.
AZRXWF	Key_mgmt=NONE for SSID = "Google Starbucks"
B4BFFC	The "Google Starbucks" wireless network does not require a psk (password). (userdata(ExtX)/Root/misc/wifi/networkHistory.txt and MSAB XRY Device Extraction Report - Device/Network Information)
BX4PD7	No
C3CNWB	No
C9GBYC	No
D37Q26	NO
D8L2EA	No password is required
DHJ3QD	No
DJFH4A	No
DRKPJA	None

TABLE 1

Question 7 - Phone & Network Settings

WebCode	Response
E3HPVE	No
EG36YD	No
EMVHN9	Wireless network, "Google Starbucks" did not require a password.
FWP664	NO
FXKN86	Password not require
G63GVA	Google Starbucks: No password
GKUDX6	NO PSK. userdata (ExtX)/Root/misc/wifi/wpa_supplicant.conf
GNTPT6	No
GQNYD8	No
GRQTE7	Simple (psk = very secret passphrase) second ssid (psk = very secret passphrase) example (psk = foobar / very secret passphrase) leap-example (psk = foobar) ikev2-example (psk = foobar) eap-fast-test (psk = password) test adhoc (psk = secret passphrase)
JZ4RHZ	No, the file located at /misc/wifi/wpa_supplicant.conf contains only the Google Starbucks SSID with no password. An example file exists at /etc/wifi/wpa_supplicant.conf that has example listings: SSID=example PSK=not so secret passphrase.
K7GAZZ	No
KGL8Y2	No. According to the wpa_supplicant.conf, eap=SIM.
KJ6YQY	Network „Google Starbucks" do not have a password.
KJNZ38	No
KNHWRY	no
KUA4A8	There are a number of ways to obtain this information, but I located a screenshot within unallocated space on the cellular device forensic image using Internet Evidence Finder (IEF). The IEF screenshot indicates that the wireless network that the device is connected to, which is GOOGLE STARBUCKS, is NOT password protected, therefore is an OPEN NETWORK. NO PASSWORD REQUIRED (KEY_MGMT = NONE)
KZFX43	No
L66WV3	none
L6LTN3	No - none
LYLK83	No
M3ZEMY	No
M9L8YY	No
MDGY8V	No
MHCT6X	No
NDV89V	No
NGBFWV	No
NUDXH3	simple- very secret passphrase second ssid- very secret passphrase example- not so secure passphrase/foobar leap-example- foobar google starbucks - none ikev2-example foobar eap-fast-test password test adhoc secret passphrase
PK8DUZ	No
QCCWH2	No
QQ8CHV	No

TABLE 1

Question 7 - Phone & Network Settings

WebCode	Response
QVK6NT	No
RGCV7W	No
RR6VHG	1-very secret passphrase 2-very secret passphrase 06b4be19da289f475aa46a33cb793029d4ab3db7a23ee92382eb0106c72ac7bb 3-# priority=2 4-not so secure passphrase 5- 6-foobar 7-foobar 8- 9-06b4be19da289f475aa46a33cb793029d4ab3db7a23ee92382eb0106c72ac7bb 10-000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f 11- 12-06b4be19da289f475aa46a33cb793029 13- 14-foobar 15-foobar 16-password 17- 18- 19- 20-secret passphrase 21-very secret passphrase, foobar 22- 23-
T8QRYW	No, none required to connect to Google Starbucks
TT8FBU	foobar,not so secure passphrase,password,secret password,very secret passphrase
UFLZ8U	The network did not require a password.
UQC6QQ	No
URBWAT	No
V2AL8P	No
VHGMPN	No Password Required
VJC6QP	No
VN3F2M	No
WWD2MW	very secret passphrase foobar password not so secure passphrase
XN3Y2V	eap-fast-test= password, leap-example= foobar, eap-psk-test= 06b4be19da289f475aa46a33cb793029, ezample= foobar
YHLTAN	none
ZKATLG	No password required. No passwords for wireless found.
ZVTJVL	none
ZWTAEN	secret passphrase, password, foobar, not so secret passphrase, versecret passphrase, foobar

TABLE 1

Question 7 - Phone & Network Settings

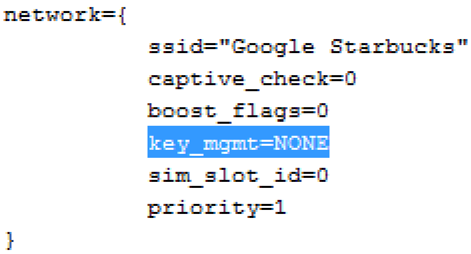
Consensus Result: No

Expected Response Explanation:

Information about wireless connections can be found in the wpa_supplicant.conf file. This file can be found at: data\misc\wifi\wpa_supplicant.conf

Expected Response Illustration:

Wireless Device Connection:

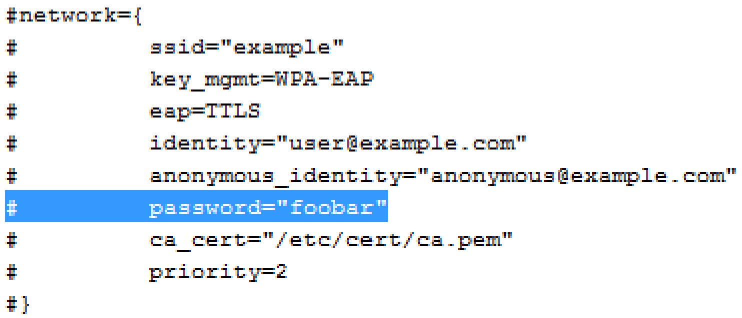


```
network={
          ssid="Google Starbucks"
          captive_check=0
          boost_flags=0
          key_mgmt=NONE
          sim_slot_id=0
          priority=1
}
```

Other Responses:

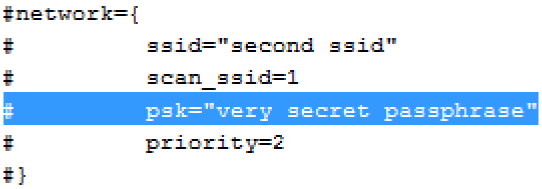
Seven participants reported responses found in the example wifi configuration supplicant file, wpa_supplicant.conf. This file can be found at:
data\etc\wifi\wpa_supplicant.conf

"Foobar" From Wifi Example Supplicant File:



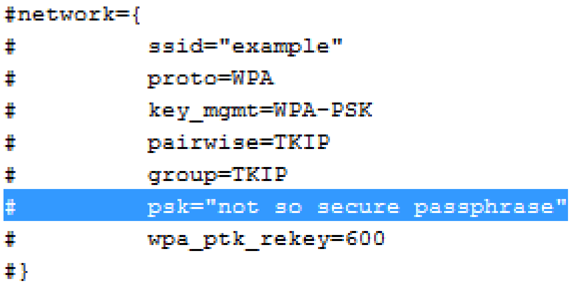
```
#network={
#         ssid="example"
#         key_mgmt=WPA-EAP
#         eap=TTLS
#         identity="user@example.com"
#         anonymous_identity="anonymous@example.com"
#         password="foobar"
#         ca_cert="/etc/cert/ca.pem"
#         priority=2
#}
```

"Very Secret Passphrase" From Wifi Example Supplicant File:



```
#network={
#         ssid="second ssid"
#         scan_ssid=1
#         psk="very secret passphrase"
#         priority=2
#}
```

"Not So Secure Passphrase" From Wifi Example Supplicant File:



```
#network={
#         ssid="example"
#         proto=WPA
#         key_mgmt=WPA-PSK
#         pairwise=TKIP
#         group=TKIP
#         psk="not so secure passphrase"
#         wpa_ptk_rekey=600
#}
```

TABLE 1

Question 8 - Phone & Network Settings

Question 8: What is the name of the Bluetooth device that this device was connected to?

Manufacturer's Expected Response: KIA Motors

WebCode	Response
2EKP2R	KIA Motors
2L4XFF	KIA MOTORS
2T3MWK	KIA MOTORS
2ZYCPH	Frosty
3XNA9L	KIA MOTORS
4EAWZL	KIA MOTORS
67DGNM	KIA MOTORS Location:[ROOT]/misc/bluedroid/bt_config.xml
6B4QXK	"KIA MOTORS"
6FZH7G	KIA MOTORS.
6JJAHK	KIA MOTORS
6KETJL	KIA MOTORS
76HXLK	KIA MOTORS
77PFKG	KIA MOTORS
7BNU7K	KIA MOTORS
7K8NDH	KIA MOTORS
8BHWAF	KIA MOTORS
8DP7RD	KIA MOTORS
9AEBRE	FROSTY
9CPE9B	KIA MOTORS
A2MFXG	KIA MOTORS
AWRL2F	KIA MOTORS
AZRXWF	KIA MOTORS
B4BFFC	KIA MOTORS. (userdata(ExtX)/Root/misc/bluedroid/bt_config.xml)
BX4PD7	FROSTY
C3CNWB	KIA MOTORS
C9GBYC	KIA Motors
D37Q26	KIA MOTORS
D8L2EA	Kia Motors
DHJ3QD	KIA MOTORS
DJFH4A	There is no record of bluetooth connections.
DRKPJA	KIA Motors Charge
E3HPVE	KIA Motors
EG36YD	Kia Motors
EMVHN9	FROSTY is the name of the phone and KIA MOTORS is the name of the Bluetooth device the phone was connected to.

TABLE 1

Question 8 - Phone & Network Settings

WebCode	Response
FWP664	KIA MOTORS
FXKN86	Not found the bluetooth connection history in "btopp.db" file.
G63GVA	Kia Motors
GKUDX6	FROSTY userdata (ExtX)/Root/data/com.android.providers.settings/databases/settings.db
GNTPT6	KIA MOTORS
GQNYD8	KIA MOTORS
GRQTE7	KIA MOTORS Charge
JZ4RHZ	KIA MOTORS
K7GAZZ	KIA MOTORS
KGL8Y2	KIA MOTORS
KJ6YQY	The name of Bluetooth device that this device was connected to is „KIA MOTORS".
KJNZ38	KIA MOTORS
KNHWRY	KIA MOTORS
KUA4A8	I navigated to the hda34 volume on the device, where there was a folder containing documentation that supports that the cellular device was connected to the following bluetooth device: - LGBluetooth4
KZFX43	KIA MOTORS
L66WV3	kia motors
L6LTN3	KIA Motors
LYLK83	10:08:C1:CF:6E:76
M3ZEMY	KIA MOTORS
M9L8YY	KIA MOTORS
MDGY8V	KIA MOTORS
MHCT6X	KIA MOTORS
NDV89V	KIA MOTORS
NGBFWV	KIA MOTORS
NUDXH3	Kia Motors MAC address (10:08:c1:cf:6e:76)
PK8DUZ	FROSTY
QCCWH2	KIA MOTORS
QQ8CHV	KIA MOTORS, Charge
QVK6NT	KIA Motors
RGCV7W	Kia Motors
RR6VHG	1-KIA MOTORS 2-Charge
T8QRYW	KIA MOTORS
TT8FBU	KIA MOTORS
UFLZ8U	KIA MOTORS
UQC6QQ	There was no record of Bluetooth devices connected to this device.
URBWAT	KIA MOTORS (The device's Bluetooth name is Frosty.)
V2AL8P	FROSTY

TABLE 1

Question 8 - Phone & Network Settings

WebCode	Response
VHGMPN	KIA MOTORS
VJC6QP	KIA MOTORS
VN3F2M	Kia Motors
WWD2MW	KIA MOTORS
XN3Y2V	Kia Motors
YHLTAN	KIA MOTORS
ZKATLG	FROSTY
ZVTJVL	KIA MOTORS
ZWTAEN	KIA MOTORS

Consensus Result: KIA Motors

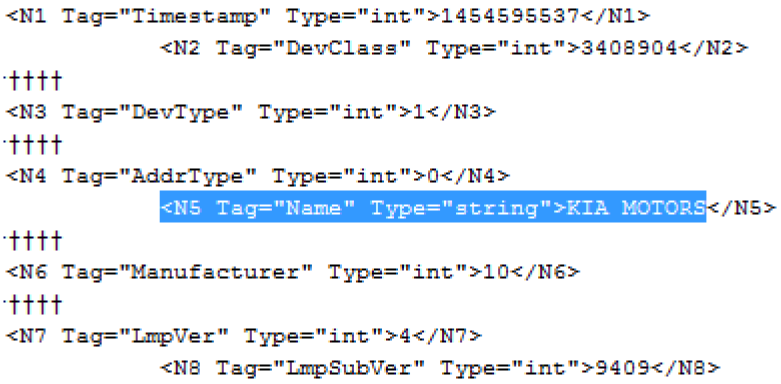
Expected Response Explanation:

The expected response is the vehicle's bluetooth device name in which this smart phone is connected to.

Information about the vehicle's bluetooth device name can be found in the bt_config.old file. This file can be found at: data\root\misc\bluedroid\bt_config.old

Expected Response Illustration:

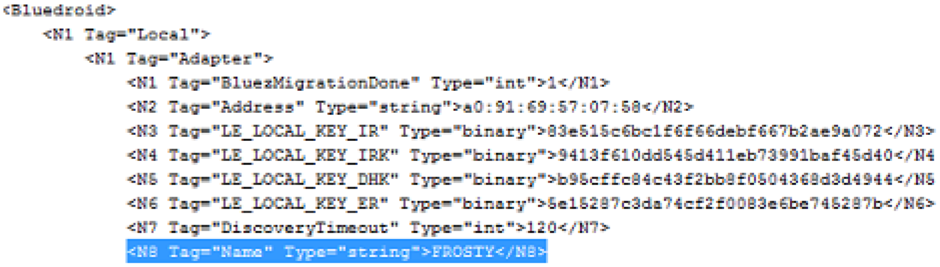
KIA Motors Bluetooth Configuration:



```
<N1 Tag="Timestamp" Type="int">1454595537</N1>
           <N2 Tag="DevClass" Type="int">3408904</N2>
·††††
<N3 Tag="DevType" Type="int">1</N3>
·††††
<N4 Tag="AddrType" Type="int">0</N4>
           <N5 Tag="Name" Type="string">KIA MOTORS</N5>
·††††
<N6 Tag="Manufacturer" Type="int">10</N6>
·††††
<N7 Tag="LmpVer" Type="int">4</N7>
           <N8 Tag="LmpSubVer" Type="int">9409</N8>
```

Other Responses:

Seven participants reported "FROSTY" which is the smart phone's bluetooth device name. Information about the smart phone's bluetooth device name can be found in the bt_config.xml file. This file can be found at: root\misc\bluedroid\bt_config.xml
Frosty Bluetooth Configuration:



```
<Bluedroid>
    <N1 Tag="Local">
        <N1 Tag="Adapter">
            <N1 Tag="BluezMigrationDone" Type="int">1</N1>
            <N2 Tag="Address" Type="string">a0:91:69:57:07:58</N2>
            <N3 Tag="LE_LOCAL_KEY_IR" Type="binary">83e515c6bc1f6f66debf667b2ae9a072</N3>
            <N4 Tag="LE_LOCAL_KEY_IRK" Type="binary">9413f610dd545d411eb73991baf45d40</N4
            <N5 Tag="LE_LOCAL_KEY_DHK" Type="binary">b95cffc84c43f2bb8f0504368d3d4944</N5
            <N6 Tag="LE_LOCAL_KEY_ER" Type="binary">5e15287c3da74cf2f0083e6be745287b</N6>
            <N7 Tag="DiscoveryTimeout" Type="int">120</N7>
            <N8 Tag="Name" Type="string">FROSTY</N8>
```

TABLE 1

Question 9 - Phone & Network Settings

Question 9: What date was the Bluetooth connection made? (ANSWER MUST BE PRESENTED AS DD-Month-YYYY; HH:MM:SS –UTC)

Manufacturer's Expected Response: 04-February-2016; 14:18:57 UTC

** No consensus achieved; Inconsistencies not highlighted **

WebCode	Response
2EKP2R	04-02-2016; 02:18:57PM UTC
2L4XFF	04-02-2016; 14:18:57 UTC
2T3MWK	04-Feb-2016; 14:18:57 (-05:00 UTC)
2ZYCPH	04/02/2016 02:18:59 UTC -5
3XNA9L	04/02/2016 14:18:57
4EAWZL	04-Februari-2016; 14:18:57 UTC
67DGNM	04/02/2016 09:18:57 AM (UTC-5:00) Location:[ROOT]/misc/bluedroid/bt_config.xml
6B4QXK	04-Feb-2016; 14:18:57 UTC
6FZH7G	04-February-2016 02:18:57 PM -0 UTC.
6JJAHK	04-02-2016; 14:18:57-UTC
6KETJL	04-February-2016 14:18:57 UTC
76HXLK	02/04/2016; 14:18:57 -0
77PFKG	04-February-2016; 02:18:57PM
7BNU7K	04/02/2016 14:18:57 -00:00
7K8NDH	04-February-2016; 14:18:57 -UTC
8BHWAF	04-02-2016; 14:18:57 -UTC
8DP7RD	(04-February-2016; 14:18:57-UTC)
9AEBRE	16.06.2015 8:41:57(UTC+0)
9CPE9B	04-February-2016; 09:18:57 (UTC-5)
A2MFXG	04-02-2016; 14:18:57 -UTC
AWRL2F	2/04/16 9:18:40 AM (UTC-5)
AZRXWF	04-February-2016; 09:18:57AM -UTC
B4BFFC	04-February-2016; 09:18:57 - UTC -05:00. (userdata(ExtX)/Root/misc/bluedroid/bt_config.xml)
BX4PD7	2/4/2016 5:50:33 PM(UTC+0)
C3CNWB	04-feb-2016; 14:18:57 -UTC
C9GBYC	04-February-2016; 09:18:57 UTC-5
D37Q26	04-February-2016; 14:18:57-UTC
D8L2EA	04-February-2016; 14:18:57 UTC
DHJ3QD	04-02-2016, 14:18:57 - UTC
DJFH4A	There is no record of bluetooth connections.
DRKPJA	04-02-2016; 14:18:57 UTC
E3HPVE	04-02-2016;09:18:57-UTC
EG36YD	04-February-2016 02:18:57 PM UTC
EMVHN9	04-February-2016; 14:18:57-UTC+0 (converted from epoch time of 1454595537)

TABLE 1

Question 9 - Phone & Network Settings

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
FWP664	04-02-2016;14:18:57 UTC
FXKN86	Not found the bluetooth connection history in "btopp.db" file.
G63GVA	04/02/2016 18:57:
GKUDX6	04-02-2016 14:18:57 KIA Motors Userdat(ExtX)/Root/misc/bluedroid/bt_config.xml
GNTPT6	04-February-2016; 14:18:57
GQNYD8	04-February-2016; 09:18:57 UTC-5
GRQTE7	KIA MOTORS = 04-Feb-16 02:18:57 PM
JZ4RHZ	04-February-2016; 09:18:57 -0500 UTC
K7GAZZ	04-Feb-2016;14:18:57
KGL8Y2	04-Feb-2016; 14:18:57 -UTC
KJ6YQY	The date was: 04.02.2016 14:18:57.
KJNZ38	04-February-2016; 09:18:57 UTC-5
KNHWRY	04-February-2016; 14:18:57-UTC
KUA4A8	I navigated to the hda34 volume on the device, where there was a folder containing documentation that supports that the cellular device was connected to the LGBluetooth4 device on June 16, 2015 at 4:41:57AM, which is based on the Last Written and Last Accessed dates. The following is the answer in the required format: - 16-JUNE-2015; 08:41:57-UTC
KZFX43	04-February-2016; 14:18:57 -UTC
L66WV3	04 February 2016 14:18:57 -UTC
L6LTN3	04-February-2016; 14:18:57 -UTC
LYLK83	Thu, 04 February 2016 14:18:59.771 UTC
M3ZEMY	02-04-2016; 09:19:15 AM -5UTC
M9L8YY	04-February-2016; 14:18:57 -UTC
MDGY8V	04 February 2016 14:18:57 (UTC +0)
MHCT6X	04-02-2016;14:18:57 -UTC
NDV89V	04-February-2016; 14:18:57-UTC
NGBFWV	04-February-2016; 14:18:57-UTC
NUDXH3	04-02-2016 09:18:57 am (utc-5) Feb 2nd, 2016
PK8DUZ	04-February-2016; 07:39:27 -0700
QCCWH2	04-FEB-2016 02:18:57 PM -UTC
QQ8CHV	KIA MOTORS : 04-02-2016; 14:18:57 - UTC
QVK6NT	04-February-2016; 14:18:57-UTC
RGCV7W	04-FEB-2016; 14:18:57 -UTC
RR6VHG	1- 04.02.2016 14:18:57 (UTC 0) 2-
T8QRYW	04-February-2016; 14:18:57 UTC-5:00
TT8FBU	04-February-2016; 14:18:57 UTC
UFLZ8U	04 Feb 2016 14:18:57 (UTC -8)
UQC6QQ	There was no record of Bluetooth devices connected to this device.
URBWAT	04-February-2016; 09:19:15 AM (-5 UTC)

TABLE 1

Question 9 - Phone & Network Settings

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
V2AL8P	04-02-2016; 04:02:15 PM -UTC
VHGMPN	04-Feb-2016; 09:18:57-UTC-5
VJC6QP	04-February-2016; 14:18:57 -UTC
VN3F2M	04-Febuary-2016; 14:18:57 UTC+0
WWD2MW	04-February-2016; 19:18:57-UTC
XN3Y2V	04-02-2016 09:18:40 AM UTC-5
YHLTAN	04/02/2016 14:18:57 UTC
ZKATLG	01/22/2016; 5:34:27 PM (UTC+0)
ZVTJVL	04-02-2016;14:18:57 -UTC
ZWTAEN	04-February-2016 14:18:57 UTC

Consensus Result: ** No consensus achieved; Inconsistencies not highlighted **

Expected Response Explanation:

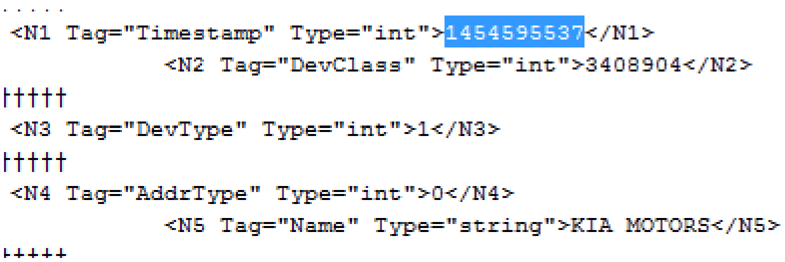
Consensus was not achieved for question 9. Majority of the responses can be placed into one group with varying conversion differences. Variations seen for this question is due to date and time conversions and response format. Below is a breakdown of the patterns seen in the responses given:

Uncoverted response for this group can be found at:
root\misc\blueroid\bt_config.old
04-February-2016; 14:18:57 UTC - 43 participants
04-Feburary-2016; 09:18:57 (UTC-5) - 9 participants
04-February-2016; 02:18:57 PM UTC - 6 participants

The value highlighted in the string contains a timestamp stored in a Unix Epoch time format which must be converted into the requested time and date format.

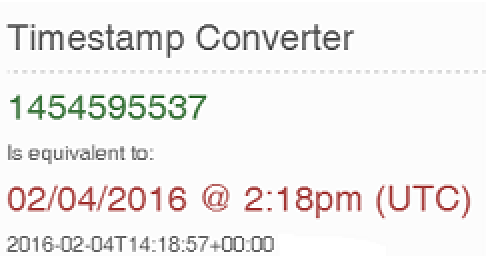
Expected Response Illustration:

Bluetooth Connection UTC Timestamp:



```
. . . . .
 <N1 Tag="Timestamp" Type="int">1454595537</N1>
           <N2 Tag="DevClass" Type="int">3408904</N2>
ŀ††††
 <N3 Tag="DevType" Type="int">1</N3>
ŀ††††
 <N4 Tag="AddrType" Type="int">0</N4>
           <N5 Tag="Name" Type="string">KIA MOTORS</N5>
ŀ++++
```

UTC Timestamp Conversion:



Timestamp Converter

1454595537

Is equivalent to:

02/04/2016 @ 2:18pm (UTC)

2016-02-04T14:18:57+00:00

TABLE 1

Question 10 - Applications

Question 10: How many calendar events are associated with this device?

Manufacturer's Expected Response: Four (4)

WebCode	Response
2EKP2R	4
2L4XFF	4
2T3MWK	4
2ZYCPH	4
3XNA9L	4
4EAWZL	4
67DGNM	Four (My 16th birthday, Dentist, Hawaii Family Vacation, T-Day) Location: [ROOT]/data/com.android.providers.calendar/databases/calendar.db
6B4QXK	4
6FZH7G	4
6JJAHK	4
6KETJL	4
76HXLK	4
77PFKG	Four
7BNU7K	4
7K8NDH	4
8BHWAF	4
8DP7RD	4
9AEBRE	4
9CPE9B	4
A2MFXG	4
AWRL2F	Four
AZRXWF	4
B4BFFC	Four (4). (Cellebrite Extraction Report - Calendar)
BX4PD7	Four calendar events
C3CNWB	4
C9GBYC	FOUR
D37Q26	4
D8L2EA	Four (4)
DHJ3QD	4
DJFH4A	4
DRKPJA	4
E3HPVE	4
EG36YD	4
EMVHN9	Four events: Hawaii Family Vacation, T-Day, Dentist, and My 16th Birthday.

TABLE 1

Question 10 - Applications

WebCode	Response
FWP664	4
FXKN86	"4 records" or "4 Events"
G63GVA	4) My 16th Birthday, Dentist, Hawaii Family Vacation, and T-Day
GKUDX6	4 userdata (ExtX)/Root/data/com.android.providers.calendar/databases/calendar.db
GNTPT6	4
GQNYD8	4
GRQTE7	12
JZ4RHZ	4 events
K7GAZZ	4
KGL8Y2	4
KJ6YQY	Four events are associated with this device.
KJNZ38	4
KNHWRY	4
KUA4A8	I navigated to the calendar directory (data/com.android.calendar), where I viewed all of the content within this folder. The calendar database file (calendar.db) was located inside of the cache folder (data/com.android.calendar/cache/calendar.db), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, it is determined that there are FOUR (4) calendar events, which are as follows: - T-DAY KEYS HIGH SCHOOL - HAWAII FAMILY VACATION - DENTIST - MY 16TH BIRTHDAY
KZFX43	Four (4)
L66WV3	4
L6LTN3	4
LYLK83	4
M3ZEMY	4
M9L8YY	4
MDGY8V	4
MHCT6X	4
NDV89V	4
NGBFWV	4
NUDXH3	4
PK8DUZ	4
QCCWH2	4
QQ8CHV	4
QVK6NT	4
RGCV7W	4
RR6VHG	4
T8QRYW	4 (Four)
TT8FBU	4
UFLZ8U	4

TABLE 1

Question 10 - Applications

WebCode	Response
UQC6QQ	4
URBWAT	4
V2AL8P	4
VHGMPN	Hawaii Family Vacation, T-Day, Dentist, My 16th Birthday
VJC6QP	4
VN3F2M	4
WWD2MW	4
XN3Y2V	Four
YHLTAN	04
ZKATLG	4
ZVTJVL	4 events
ZWTAEN	4

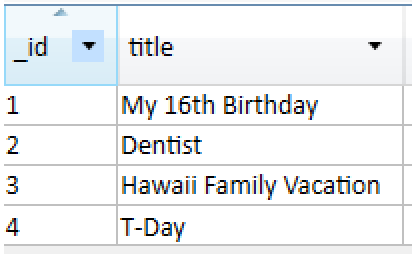
Consensus Result: Four (4)

Expected Response Explanation:

Information on calendar events can be found in the calendar.db database. The events table will show all calendar events. The file can be found at:
\data\com.android.providers.calendar\databases\calendar.db

Expected Response Illustration:

Database: calendar >>> Table: events



_id	title
1	My 16th Birthday
2	Dentist
3	Hawaii Family Vacation
4	T-Day

TABLE 1

Question 11 - Applications

Question 11: What are the memos(names) of the Alarms set on this device?

Manufacturer's Expected Response: Wake-up
Revenge

WebCode	Response
2EKP2R	Wake Up Revenge
2L4XFF	Acappella_Good_Morning, Afternoon_Walk, Alarm_1, Alarm_2, Beautiful_Day, Cello, Clockwork, Country_Road, Dawning_Sky, Lifes_Good_Alarm, Morning_Scent, Running, Shampoo, Timer, Trumpet, Voice_of_Nature, Weather_Forecast, West_Winds.
2T3MWK	Wake-up Revenge
2ZYCPH	My 16th Birthday, Dentist, Hawaii Family Vacation, T-Day
3XNA9L	Wake-ip , Revenge
4EAWZL	Wake-up Revenge
67DGNM	Wake-up Revenge
6B4QXK	"Wake-up" and "Revenge"
6FZH7G	Wake-up and Revenge.
6JJAHK	Wake-up Revenge Wake-up is enabled, Revenge is not enabled.
6KETJL	wake-up revenge
76HXLK	Wake-up and Revenge
77PFKG	Revenge, Wake-up
7BNU7K	Wake-up Revenge
7K8NDH	Wake-up Revenge
8BHWAF	Wake-up Revenge
8DP7RD	Wake-up Revenge
9AEBRE	Wake-up, Revenge
9CPE9B	Wake-Up Revenge
A2MFXG	Wake-up, Revenge
AWRL2F	Wake-up Revenge
AZRXWF	Wake-up, Revenge
B4BFFC	There were two (2) memos(names) of the Alarms. They were named the following: "Wake-up" and "Revenge". (alarms.db, Alarms table)
BX4PD7	Wake-up Revenge
C3CNWB	Wake-up Revenge
C9GBYC	Wake-up and Revenge
D37Q26	REVENGE WAKE-UP
D8L2EA	Wake-up Revenge
DHJ3QD	My 16th Birthday Dentist Hawaii Family Vacation T-Day
DJFH4A	Wake-up and Revenge
DRKPJA	Wake-up Revenge
E3HPVE	Wake-up Revenge
EG36YD	Wake-up; Revenge

TABLE 1

Question 11 - Applications

WebCode	Response
EMVHN9	Two alarms named, Wake-up and Revenge.
FWP664	My 16th Birthday, Dentist, T-Day, Hawaii Family Vacation
FXKN86	"Wake-up" and "Revenge"
G63GVA	Wake-up Thursday, February 4 06:45 Revenge
GKUDX6	Wake-up Revenge userdata (ExtX)/Root/data/com.lge.clock/databases/alarms.db
GNTPT6	Wake-up Revenge
GQNYD8	Dentist T-Day
GRQTE7	1-My 16th Birthday 2-Dentist 3-Hawaii Family Vacation 4-T-Day
JZ4RHZ	Wake-up and Revenge
K7GAZZ	Wake-Up, Revenge
KGL8Y2	Wake-up Revenge
KJ6YQY	The memos (names) of the Alarms set on this device are: Wake-up, Revenge.
KJNZ38	Wake-up Revenge
KNHWRY	Wake-up and Revenge
KUA4A8	I navigated to the memo directory (data/com.lge.qmemoplus), where I viewed all of the content within this folder. The qmemoplus database file (qmemoplus.db) was located inside of the shared_prefs folder (data/com.lge.qmemoplus/shared_prefs/qmemoplus.db), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, it is determined that there are THREE (3) memos, which are as follows: - MUSIC: The Coasters The Delfonics Bobby Womack The George Baker Selection - GROCERY LIST: Chips Soda Fruit Snacks Peanut Butter - TARGETS: Lisa Hilary Diane Principal Skinner
KZFX43	Wake-up, Revenge
L66WV3	Wake-up Revenge
L6LTN3	Wake-up Revenge
LYLK83	Wake-up, Revenge
M3ZEMY	Wake-up Revenge
M9L8YY	Wake-up Revenge
MDGY8V	Wake-up and Revenge
MHCT6X	Wake-up and Revenge
NDV89V	Wake-up and Revenge
NGBFWV	Wake-up, Revenge
NUDXH3	Wake-Up, Revenge
PK8DUZ	Hawaii Family Vacation, Dentist, My 16th birtday, T-DayKeys High School
QCCWH2	WAKE-UP
QQ8CHV	Revenge, Wake-up
QVK6NT	Wake-up Revenge
RGCV7W	Wake-up, and Revenge
RR6VHG	1-Hawaii Family Vacation (Passive) 2-T-Day (Active) 3-Dentist (Active) 4-My 16th Birthday (Passive)
T8QRYW	Wake-up Revenge

TABLE 1

Question 11 - Applications

WebCode	Response
TT8FBU	Wake-up,Revenge
UFLZ8U	"Wake-up" and "Revenge"
UQC6QQ	Wake-up and Revenge
URBWAT	Wake-up Revenge
V2AL8P	Wake-up Revenge
VHGMPN	Wake-up, Revenge
VJC6QP	Revenge Wake-up
VN3F2M	Wake-up Revenge
WWD2MW	Wake-up Revenge
XN3Y2V	wake up Revenge
YHLTAN	Wake-up Revenge
ZKATLG	Hawaii Family Vacation, T-Day, Dentist, My 16th Birthday
ZVTJVL	Wake-up Revenge
ZWTAEN	Wake-up, Revenge

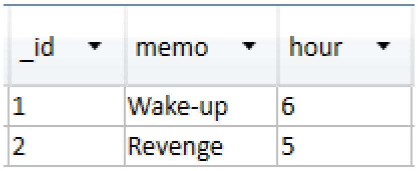
Consensus Result: Wake-up
Revenge

Expected Response Explanation:

Information for alarms can be found in the alarms.db database. The alarms table will contain the alarm memo. The file can be found at:
\data\com.lge.clock\databases\alarms.db

Expected Response Illustration:

Database: alarms >>> Table: alarms



_id	memo	hour
1	Wake-up	6
2	Revenge	5

Other Responses:

Eight participants reported the four calendar events that are associated with this device. The calendar events can be found in the calendar database. The file can be found at:
\data\com.android.providers.calendar\databases\calendar.db

TABLE 1

Question 12 - Applications

Question 12: List the first third-party application to be downloaded onto the device. (ANSWERS MUST HAVE BOTH THE “package_name” and “title")

Manufacturer's Expected Response: Package_name: "Com.tumblr"
Title: "Tumblr"

WebCode	Response
2EKP2R	Tumblr com.tumblr
2L4XFF	Tumblr com.tumblr
2T3MWK	Package_name: com.tumblr Title: Tumblr
2ZYCPH	"com.tumblr" "Tumblr"
3XNA9L	com.tumblr Tumblr
4EAWZL	com.tumblr Tumblr
67DGNM	package name: com.tumbler Title: Tumblr
6B4QXK	"com.tumblr” and “Tumblr”
6FZH7G	com.tumblr Tumblr
6JJAHK	package_name: com.tumblr title: Tumblr
6KETJL	package_name: com.tumblr title: Tumblr
76HXLK	Tumblr - com.tumblr
77PFKG	com.tumblr / Tumblr
7BNU7K	com.tumblr Tumblr
7K8NDH	(com.tumblr) Tumblr
8BHWAF	com.tumblr Tumblr
8DP7RD	Tumblr com.tumblr
9AEBRE	com.tumblr, Tumblr
9CPE9B	com.tumblr tumblr
A2MFXG	com.tumblr, Tumblr
AWRL2F	Tumblr com.tumblr
AZRXWF	com.tumblr Tumblr
B4BFFC	package_name: com.tumblr, title: Tumblr. (localappstate.db, Appstate table, and Cellebrite Extraction Report - Installed Applications)
BX4PD7	Com.tumblr is the package name and Tumblr is the title.
C3CNWB	package_name : com.tumblr title : Tumblr
C9GBYC	package_name: com.tumblr title: Tumblr
D37Q26	package_name com.tumblr title: tumblr
D8L2EA	Tumblr Package name: com.tumblr
DHJ3QD	com.tumblr Tumblr
DJFH4A	Tumblr com.tumblr
DRKPJA	com.tumblr-1 Tumblr
E3HPVE	"package_name" = com.tumblr "title" = Tumblr
EG36YD	com.tumblr, Tumblr
EMVHN9	Com.tumblr, Tumblr

TABLE 1

Question 12 - Applications

WebCode	Response
FWP664	com.tumblr, Tumblr
FXKN86	Package Name: com.microsoft.office.lync15 Title Name: don't have
G63GVA	Package_name=com.tumblr title=Tumblr Package_name=com.microsoft.office.lync15 title=Skype for Business for Android Package_name=com.skype.raider title=Skype - free IM & video calls
GKUDX6	Com.Tumblr package name Tumblr title
GNTPT6	com.tumblr, Tumblr
GQNYD8	com.tumblr Tumblr
GRQTE7	Tumblr / com.tumblr
JZ4RHZ	com.tumblr, Tumblr
K7GAZZ	"base.apk", "tumblr"
KGL8Y2	"package_name" com.tumblr "title" Tumblr
KJ6YQY	package_name :”com.tumblr” and title: ” Tumblr”.
KJNZ38	com.tumblr Tumblr
KNHWRY	com.tumblr Tumblr
KUA4A8	Based on the analysis of the installed third-party applications, it was determined that Tumblr was the first to be downloaded on the device. The following is the answer in the required format: - "package_name" = com.tumblr-1 - "title" = Tumblr - 22-January-2016; 12:33:37PM (4:33:37-UTC)
KZFX43	Title: Tumblr Package Name: com.tumblr
L66WV3	com.tumblr Tumblr
L6LTN3	Tumblr com.tumblr
LYLK83	com.tumblr Tumblr
M3ZEMY	com.tumblr Tumblr
M9L8YY	com.skype.raider Skype - free IM & video calls
MDGY8V	The first purchased third-party application was Package: com.tumbler, Title: Tumblr,
MHCT6X	com.tumblr Tumblr
NDV89V	com.tumblr Tumblr
NGBFWV	package_name: com.tumblr title: Tumblr
NUDXH3	com.microsoft.office.lync15-1 Skype (for business)
PK8DUZ	com.tumblr&version Code=105020006 tumblr
QCCWH2	"data@app@com.tumblr-1@base.apk@classes.dex" "Tumblr"
QQ8CHV	com.tumblr, Tumblr
QVK6NT	Com.tumblr Tumblr
RGCV7W	tumblr.com, tumblr
RR6VHG	Base.apk - Tumblr
T8QRYW	Package_name is “base.apk” Title is “Tumblr”
TT8FBU	Tumblr, com.tumblr
UFLZ8U	“package_name” is com.tumblr. "title" is Tumblr.
UQC6QQ	Tumblr com.tumblr

TABLE 1

Question 12 - Applications

WebCode	Response
URBWAT	Package Name: com.tumblr Title: Tumblr
V2AL8P	package_name = com.tumblr title = Tumblr
VHGMPN	"com.tumblr" – "Tumblr"
VJC6QP	com.tumblr Tumblr
VN3F2M	com.tumblr Tumblr
WWD2MW	Tumblr com.tumblr
XN3Y2V	com.Tumblr Tumblr
YHLTAN	"com.android.chrome" chrome "com.facebook.orca" MESSANGER "com.facebook.katana" facebook "com.instagram.android" instagram. "com.skype.raider"skype "com.microsoft.office.lync15" microsoft.office. "com.tumblr" tumblr
ZKATLG	Com.tumblr-1, Tumblr
ZVTJVL	package_name:com.tumblr tittle :Tumblr
ZWTAEN	Tumblr com.tumblr

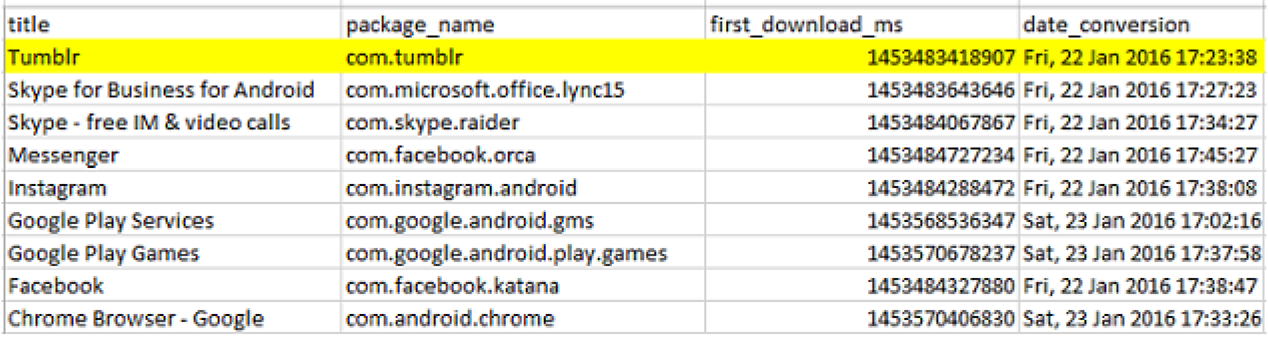
Consensus Result: Com.tumblr (Tumblr)

Expected Response Explanation:

To determine the first third-party application downloaded onto this device participants needed to convert the Unix Epoch timestamp values listed in the "first_download_ms" column found within the appstate table of the localappstore.db database. The value for Tumblr is 1453483418907. The localappstate.db database can be found at: data\com.android.vending\databases\localappstate.db

Expected Response Illustration:

Database: localappstate >>> Table: appstate



title	package_name	first_download_ms	date_conversion
Tumblr	com.tumblr	1453483418907	Fri, 22 Jan 2016 17:23:38
Skype for Business for Android	com.microsoft.office.lync15	1453483643646	Fri, 22 Jan 2016 17:27:23
Skype - free IM & video calls	com.skype.raider	1453484067867	Fri, 22 Jan 2016 17:34:27
Messenger	com.facebook.orca	1453484727234	Fri, 22 Jan 2016 17:45:27
Instagram	com.instagram.android	1453484288472	Fri, 22 Jan 2016 17:38:08
Google Play Services	com.google.android.gms	1453568536347	Sat, 23 Jan 2016 17:02:16
Google Play Games	com.google.android.play.games	1453570678237	Sat, 23 Jan 2016 17:37:58
Facebook	com.facebook.katana	1453484327880	Fri, 22 Jan 2016 17:38:47
Chrome Browser - Google	com.android.chrome	1453570406830	Sat, 23 Jan 2016 17:33:26

TABLE 1

Question 13 - Applications

Question 13: What term(s) were searched for in the Google Play Store?

Manufacturer's Expected Response: tumblr

WebCode	Response
2EKP2R	Tumblr
2L4XFF	tumblr
2T3MWK	tumblr
2ZYCPH	tumblr
3XNA9L	tumblr
4EAWZL	tumblr
67DGNM	tumblr
6B4QXK	tumblr
6FZH7G	tumblr
6JJAHK	tumblr
6KETJL	tumblr
76HXLK	Tumblr
77PFKG	tumblr
7BNU7K	tumblr
7K8NDH	tumblr
8BHWAF	tumblr
8DP7RD	tumblr
9AEBRE	tumblr
9CPE9B	tumblr
A2MFXG	tumblr
AWRL2F	tumblr
AZRXWF	Tumblr
B4BFFC	tumblr. (Cellebrite Extraction Report - Searched Items)
BX4PD7	Tumblr
C3CNWB	Tumblr
C9GBYC	tumblr
D37Q26	tumblr
D8L2EA	tumblr
DHJ3QD	tumblr
DJFH4A	tumblr
DRKPJA	Yahoo mail
E3HPVE	tumblr
EG36YD	tumblr
EMVHN9	tumblr
FWP664	tumblr

TABLE 1

Question 13 - Applications

WebCode	Response
FXKN86	"facebook", "microsoft office" and "games"
G63GVA	tumblr
GKUDX6	Tumblr userdata (ExtX)/Root/data/com.android.vending/databases/suggestions.db
GNTPT6	tumblr
GQNYD8	Tumblr
GRQTE7	known
JZ4RHZ	tumblr
K7GAZZ	tumblr
KGL8Y2	tumblr
KJ6YQY	”tumblr”
KJNZ38	Tumblr
KNHWRY	tumblr
KUA4A8	Based on the analysis of the installed third-party applications (data/app), it was determined that the following were downloaded to the device: - Tumblr - Microsoft Office - Skype (Raider) - Instagram - Facebook (Katana) - Facebook Messenger (Orca)
KZFX43	tumblr
L66WV3	tumblr
L6LTN3	tumblr
LYLK83	Tumblr
M3ZEMY	tumblr
M9L8YY	tumblr
MDGY8V	tumblr
MHCT6X	tumblr
NDV89V	tumblr
NGBFWV	tumblr
NUDXH3	tumblr
PK8DUZ	tumblr
QCCWH2	tumblr
QQ8CHV	tumblr
QVK6NT	Tumblr
RGCV7W	tumblr
RR6VHG	Tumblr
T8QRYW	tumblr
TT8FBU	tumblr
UFLZ8U	tumblr
UQC6QQ	tumblr
URBWAT	tumblr
V2AL8P	tumblr

TABLE 1

Question 13 - Applications

WebCode	Response
VHGMPN	tumblr
VJC6QP	tumblr
VN3F2M	Tumblr
WWD2MW	tumblr
XN3Y2V	Tumblr
YHLTAN	
ZKATLG	tumblr
ZVTJVL	tumblr
ZWTAEN	Tumblr

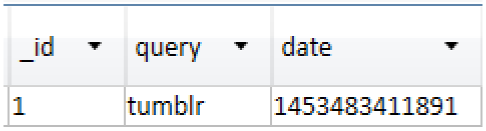
Consensus Result: tumblr

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 the queries that were searched for. This file can be found at: data\com.android.vending\databases\suggestions.db.

Expected Response Illustration:

Database: suggestions >>> Table: suggestions



_id	query	date
1	tumblr	1453483411891

TABLE 1

Question 14 - Applications

Question 14: What is the blog name for the Tumblr account associated with this device?

Manufacturer's Expected Response: torturedteenagesoul88

WebCode	Response
2EKP2R	torturedteenagesoul88
2L4XFF	torturedteenagesoul88torturedteenagesoul88.tumblr.com
2T3MWK	torturedteenagesoul88
2ZYCPH	torturedteenagesoul88
3XNA9L	torturedteenagesoul88
4EAWZL	torturedteenagesoul88
67DGNM	tourturedteenagesoul88
6B4QXK	torturedteenagesoul88
6FZH7G	Torturedteenagesoul88
6JJAHK	torturedteenagesoul88
6KETJL	torturedteenagesoul88
76HXLK	torturedteenagesoul88
77PFKG	torturedteenagesoul88
7BNU7K	torturedteenagesoul88
7K8NDH	torturedteenagesoul88
8BHWAF	torturedteenagesoul88
8DP7RD	torturedteenagesoul88
9AEBRE	torturedteenagesoul88.tumblr.com
9CPE9B	torturedteenagesoul88
A2MFXG	torturedteenagesoul88
AWRL2F	http://torturedteenagesoul88.tumblr.com/
AZRXWF	torturedteenagesoul88
B4BFFC	torturedteenagesoul88. (Cellebrite Extraction Report - User Accounts)
BX4PD7	Torturedteenagesoul88.tumblr.com
C3CNWB	torturedteenagesoul88
C9GBYC	torturedteenagesoul88
D37Q26	torturedteenagesoul88
D8L2EA	Untitled
DHJ3QD	torturedteenagesoul88
DJFH4A	torturedteenagesoul88
DRKPJA	torturedteenagesoul88
E3HPVE	torturedteenagesoul88
EG36YD	tourturedteenagesoul88
EMVHN9	torturedteenagesoul88
FWP664	torturedteenagesoul88

TABLE 1

Question 14 - Applications

WebCode	Response
FXKN86	torturedteenagesoul88
G63GVA	torturedteenagesoul88
GKUDX6	Torturedteenagesoul88 userdata (ExtX)/Root/data/com.tumblr/databases/Tumblr.sqlite
GNTPT6	torturedteenagesoul88
GQNYD8	torturedteenagesoul88
GRQTE7	torturedteenagesoul88.tumblr.com
JZ4RHZ	torturedteenagesoul88.tumblr.com
K7GAZZ	torturedteenagesoul88
KGL8Y2	untitled
KJ6YQY	The blog name is „torturedteenagesoul88".
KJNZ38	torturedteenagesoul88
KNHWRY	torturedteenagesoul88
KUA4A8	I navigated to the Tumblr directory (data/com.tumblr), where I viewed all of the content within this folder. A Tumblr database file (tumblr.sqlite) was located inside of the shared_prefs folder (com.tumblr/shared_prefs/tumblr.sqlite), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, it is determined that the blog name for the Tumblr account is as follows: - torturedteenagesoul88.tumblr.com
KZFX43	torturedteenagesoul88
L66WV3	torturedteenagesoul88
L6LTN3	torturedteenagesoul88
LYLK83	torturedteenagesoul88
M3ZEMY	torturedteenagesoul88
M9L8YY	torturedteenagesoul88
MDGY8V	torturedteenagesoul88
MHCT6X	torturedteenagesoul88
NDV89V	torturedteenagesoul88
NGBFWV	torturedteenagesoul88
NUDXH3	Torturedteenagesoul88
PK8DUZ	torturedteenagersoul88
QCCWH2	torturedteenagesoul88.tumblr.com
QQ8CHV	torturedteenagesoul88
QVK6NT	torturedteenagesoul88
RGCV7W	tourturedteenagesoul88
RR6VHG	torturedteenagesoul88
T8QRYW	torturedteenagesoul88
TT8FBU	torturedteenagesoul88
UFLZ8U	torturedteenagesoul88
UQC6QQ	torturedteenagesoul88

TABLE 1

Question 14 - Applications

WebCode	Response
URBWAT	torturedteenagesoul88
V2AL8P	torturedteenagesoul88
VHGMPN	torturedteenagesoul88
VJC6QP	torturedteenagesoul88
VN3F2M	Torturedteenagesoul88
WWD2MW	tourturedteenagesoul88
XN3Y2V	torturedteenagesoul88
YHLTAN	torturedteenagesoul88.tumblr.com
ZKATLG	Torturedteenagesoul88
ZVTJVL	torturedteenagesoul88
ZWTAEN	torturedteenagesoul88

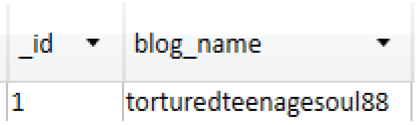
Consensus Result: torturedteenagesoul88

Expected Response Explanation:

Information about the Tumblr blog name can be found in the tumblr.sqlite database. The outbound_posts table has a blog_name section showing the primary blog name for this device. The file can be found at:
\data\com.tumblr\databases\tumblr.sqlite

Expected Response Illustration:

Database: tumblr.sqlite >>> Table: outbound_posts



_id	blog_name
1	torturedteenagesoul88

TABLE 1

Question 15 - Applications

Question 15: What is the title and content of the body for the first Tumblr post created by a user with this device?

<u>Manufacturer's Expected Response</u>: Title: "Thoughts"
Contents of Body: "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…"

WebCode	Response
2EKP2R	Mon Feb 01 10:02 EST: Title is "Thoughts", body: "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me..."
2L4XFF	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
2T3MWK	Title: Thoughts Content: Why are girls so mean? U can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
2ZYCPH	Thought- "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me.."
3XNA9L	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
4EAWZL	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
67DGNM	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me… Location: [ROOT]/data/com.tumblr/databases/Tumblr.sqlite
6B4QXK	Title: “Thoughts”; Content: “Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...”
6FZH7G	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
6JJAHK	title: Thoughts body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
6KETJL	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
76HXLK	Title :Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
77PFKG	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…

TABLE 1

Question 15 - Applications

WebCode	Response
7BNU7K	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
7K8NDH	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
8BHWAF	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
8DP7RD	Thoughts Text: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
9AEBRE	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
9CPE9B	thoughts Why are girls so mean? There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me ...
A2MFXG	Thoughts "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me..."
AWRL2F	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
AZRXWF	"Thoughts" Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
B4BFFC	Title: Thoughts Content of the Body of the Post: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me... (MSAB XRY Extraction Report - Message/Status Updates and Cellebrite Extraction Report - Tumblr Instant Messages)
BX4PD7	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
C3CNWB	Title : Thoughts Content : Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
C9GBYC	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
D37Q26	title Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me........
D8L2EA	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
DHJ3QD	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...

TABLE 1

Question 15 - Applications

WebCode	Response
DJFH4A	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
DRKPJA	Recommended for you
E3HPVE	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them in the face, but I know I can't. I just wish someone understood me...
EG36YD	Thoughts. Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
EMVHN9	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
FWP664	Title:Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
FXKN86	Title: "Feelings" Body: "I was suspended because girls were making fun of me! They were not punished and I was because I tried to stand up for myself! Now they will not leave me alone. I need help, they can't continue to get away with this!"
G63GVA	Thoughts
GKUDX6	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me… userdata (ExtX)/Root/data/com.tumblr/databases/Tumblr.sqlite-journal
GNTPT6	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them in the face, but I know that I can't. I just wish someone understood me...
GQNYD8	Thoughts "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the faces, but I know that I can't. I just wish someone understood me..."
GRQTE7	Feelings: I was suspended because girls were making fun of me! They were not punished and I was because I tried to stand up for myself! Now they will not leave me alone. I need help, they can't continue to get away with this!
JZ4RHZ	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
K7GAZZ	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
KGL8Y2	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
KJ6YQY	Title was: „Thoughts”. Content of the body was: „Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...”

TABLE 1

Question 15 - Applications

WebCode	Response
KJNZ38	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them in the face, but I know that I can't. I just wish someone understood me...
KNHWRY	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
KUA4A8	I navigated to the Tumblr directory (data/com.tumblr), where I viewed all of the content within this folder. A Tumblr database file (tumblr.sqlite) was located inside of the cache folder (com.tumblr/cache/tumblr.sqlite), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, the title and content of the first Tumblr post created by the user was as follows: - Feelings (Title) - I was suspended because girls were making fun of me! They were not punished and I was because I tried to stand up for myself! Now they will not leave me alone. I need help, they can't continue to get away with this! (Body)
KZFX43	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
L66WV3	Thoughts/ Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
L6LTN3	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
LYLK83	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
M3ZEMY	Title: thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
M9L8YY	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
MDGY8V	Title: Thoughts Body: "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…"
MHCT6X	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
NDV89V	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
NGBFWV	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
NUDXH3	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me....

TABLE 1

Question 15 - Applications

WebCode	Response
PK8DUZ	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me... published yes 0 0 0 0 0 1 -1 0 0 0 0 -1 rich 0 0 0 0 1 0 0 0 0 0 0 1 -1 -1 -1 Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me... 0
QCCWH2	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
QQ8CHV	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
QVK6NT	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
RGCV7W	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
RR6VHG	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
T8QRYW	Title = Thoughts Content of the body Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
TT8FBU	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know I can't. I just wish someone understood me...
UFLZ8U	"Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me..."
UQC6QQ	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
URBWAT	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
V2AL8P	Title = Thoughts Content of the body = Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
VHGMPN	Thoughts - Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
VJC6QP	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
VN3F2M	Title: Thoughts Body: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I wish someone understood me ...

TABLE 1

Question 15 - Applications

WebCode	Response
WWD2MW	Title: Thoughts Content: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
XN3Y2V	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
YHLTAN	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...
ZKATLG	Thoughts Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…
ZVTJVL	Title: Thoughts Text: Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't.
ZWTAEN	Thoughts: Why are girls so mean I can't stand going to school and not have been suspended because of these girls. There are times I just want to punch them all in the face but I know that I can't. I just wish someone understood me...

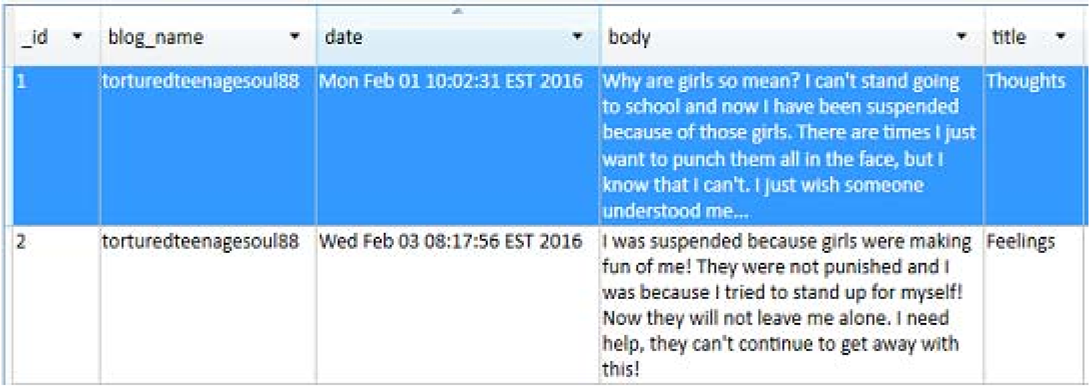
Consensus Result: Title: "Thoughts"
Body: "Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me…"

Expected Response Explanation:

Information about Tumblr posts can be found in the tumblr.sqlite database. The outbound_posts table show the content of the posts. The file can be found at:
\data\com.tumblr\databases\tumblr.sqlite

Expected Response Illustration:

Database: tumblr.sqlite >>> Table:outbound_posts



_id	blog_name	date	body	title
1	torturedteenagesoul88	Mon Feb 01 10:02:31 EST 2016	Why are girls so mean? I can't stand going to school and now I have been suspended because of those girls. There are times I just want to punch them all in the face, but I know that I can't. I just wish someone understood me...	Thoughts
2	torturedteenagesoul88	Wed Feb 03 08:17:56 EST 2016	I was suspended because girls were making fun of me! They were not punished and I was because I tried to stand up for myself! Now they will not leave me alone. I need help, they can't continue to get away with this!	Feelings

TABLE 1

Question 16 - Applications

Question 16: What is the identifier name of the external user that communicates with the active Tumblr account on this device?

Manufacturer's Expected Response: lazystranger63

WebCode	Response
2EKP2R	lazystranger63
2L4XFF	Lazystranger63.tumblr.com
2T3MWK	lazystranger63
2ZYCPH	lazystranger63
3XNA9L	Lazystranger63
4EAWZL	lazystranger63.tumblr.com
67DGNM	lazystranger63.tumblr.com
6B4QXK	lazystranger63.tumblr.com
6FZH7G	lazystranger63
6JJAHK	Lazystranger63.tumbler.com
6KETJL	lazystranger63.tumblr.com
76HXLK	lazystranger63.tumblr.com
77PFKG	lazystranger63.tumblr.com
7BNU7K	Lex Luther
7K8NDH	lazystranger63.tumblr.com
8BHWAF	lazystranger63.tumblr.com
8DP7RD	Lex Luther
9AEBRE	lazystranger63.tumblr.com
9CPE9B	lazystranger63
A2MFXG	lazystranger63.tumblr.com
AWRL2F	blackserpent34@gmail.com Lex Luther
AZRXWF	lazystranger63
B4BFFC	lazystranger63; the identifier name associated with this Tumblr account name was: Lex Luther. (Tumblr.sqlite, Messaging_message Table)
BX4PD7	Lazystranger63.tumblr.com
C3CNWB	Lazystranger63
C9GBYC	LazyStranger63
D37Q26	lazystranger63.tumblr.com
D8L2EA	lazystranger63.tumblr.com
DHJ3QD	lazystranger63.tumblr.com
DJFH4A	Lex Luther
DRKPJA	lazystranger63
E3HPVE	Stella Frost
EG36YD	Lazystranger63.tumblr.com

TABLE 1

Question 16 - Applications

WebCode	Response
EMVHN9	lazystranger63
FWP664	lazystranger63.tumblr.com
FXKN86	lazystranger63.tumblr.com
G63GVA	lazystranger63.tumblr.com
GKUDX6	Lazystranger63.tumblr.com userdata (ExtX)/Root/data/com.tumblr/databases/Tumblr.sqlite
GNTPT6	lazystranger63
GQNYD8	lazystranger63.tumblr.com
GRQTE7	lazystranger63.tumblr.com
JZ4RHZ	lazystranger63.tumblr.com
K7GAZZ	lazystranger63.tumblr.com
KGL8Y2	lazystranger63
KJ6YQY	Identifier name of the external user is: „Lex Luther”.
KJNZ38	Lex Luther
KNHWRY	Lazystranger63.tumblr.com
KUA4A8	I navigated to the Tumblr directory (data/com.tumblr), where I viewed all of the content within this folder. A Tumblr database file (tumblr.sqlite) was located inside of the shared_prefs folder (com.tumblr/shared_prefs/tumblr.sqlite), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, it is determined that the identifier name of the external user that communicates with the active Tumblr account is as follows: - torturedteenagesoul88 - (Stella Frost)
KZFX43	lazystranger63.tumblr.com
L66WV3	lazystranger63
L6LTN3	lazystranger63.tumblr.com
LYLK83	lazystranger63.tumblr.com
M3ZEMY	lazystranger63.tumblr.com
M9L8YY	lazystranger63
MDGY8V	lazystranger63.tumbler.com
MHCT6X	lazystranger63.tumblr.com
NDV89V	Lazystranger63.tumblr.com
NGBFWV	lazystranger63
NUDXH3	Lex Luther Blackserpent34@gmail.com
PK8DUZ	lazystranger63.tumblr.com
QCCWH2	lazystranger63.tumblr.com
QQ8CHV	lazystranger63
QVK6NT	Lazystranger63.tumblr.com
RGCV7W	Lazystranger63
RR6VHG	lazystranger63.tumblr.com
T8QRYW	Lazystranger63.tumblr.com
TT8FBU	Lex Luther

TABLE 1

Question 16 - Applications

WebCode	Response
UFLZ8U	Lazystranger63.tumblr.com
UQC6QQ	Lex Luther
URBWAT	lazystranger63.tumblr.com
V2AL8P	lazystranger63.tumblr.com
VHGMPN	lazystranger63.tumblr.com
VJC6QP	lazystranger63.tumblr.com
VN3F2M	Lazystranger63.tumblr.com
WWD2MW	lazystranger63
XN3Y2V	Lex Luther
YHLTAN	lazystranger63.tumblr.com
ZKATLG	Lex Luther, blackserpent34@gmail.com
ZVTJVL	lazystranger63
ZWTAEN	Lex Luthor, blackserpent34@gmail.com

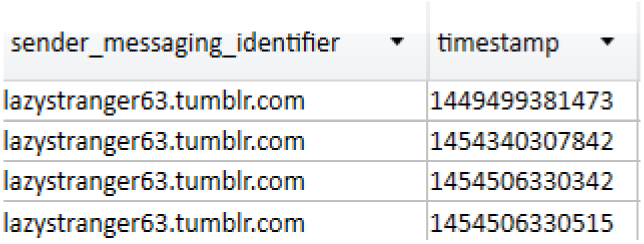
Consensus Result: lazystranger63

Expected Response Explanation:

Information about Tumblr posts can be found in the tumblr.sqlite database. The messaging_messages table identifies users who are communicating with torturedteenagesoul88. The file can be found at: data\com.tumblr\databases\tumblr.sqlite

Expected Response Illustration:

Database: tumblr.sqlite >>> Table: messaging_messages

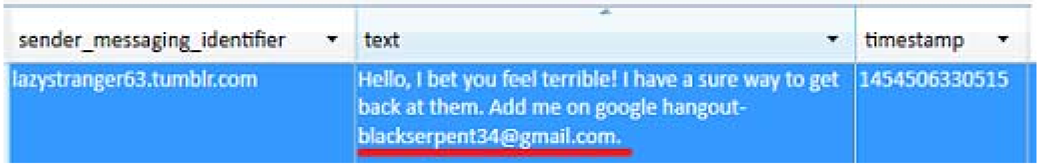


sender_messaging_identifier	timestamp
lazystranger63.tumblr.com	1449499381473
lazystranger63.tumblr.com	1454340307842
lazystranger63.tumblr.com	1454506330342
lazystranger63.tumblr.com	1454506330515

Other Responses:

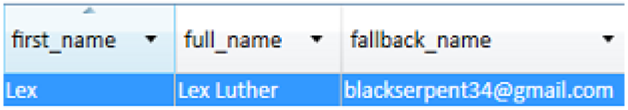
Twelve participants reported Lex Luther. These participants went outside of tumblr to determine the person associated with the username provided in a tumblr message from lazystranger63. To determine Lex Luther these participants navigated to the the Babel1 database file within the com.google.android.talk folder and viewed the participant table. Lex Luther is identified along with his Google e-mail address blackserpent34@gmail.com. The file can be found at: \data\com.google.android.talk\databases\babel1.db.

Tumblr Message Containing Google E-mail Address:



sender_messaging_identifier	text	timestamp
lazystranger63.tumblr.com	Hello, I bet you feel terrible! I have a sure way to get back at them. Add me on google hangout-blackserpent34@gmail.com.	1454506330515

Database: babel1 >>> Table: participant



first_name	full_name	fallback_name
Lex	Lex Luther	blackserpent34@gmail.com

TABLE 1

Question 17 - Applications

Question 17: What is lazystranger63's google hangout account username? (Provide full username as it is presented in the comment)

Manufacturer's Expected Response: blackserpent34@gmail.com

WebCode	Response
2EKP2R	blackserpent34@gmail.com
2L4XFF	Lex Luther
2T3MWK	blackserpent34@gmail.com
2ZYCPH	blackserpent34@gmail.com
3XNA9L	blackserpent34@gmail.com
4EAWZL	blackserpent34@gmail.com
67DGNM	Lex Luther – blackserpent34@gmail.com
6B4QXK	blackserpent34@gmail.com
6FZH7G	blackserpent34@gmail.com
6JJAHK	blackserpent34@gmail.com
6KETJL	blackserpent34@gmail.com
76HXLK	blackserpent34
77PFKG	blackserpent34@gmail.com
7BNU7K	blackserpent34@gmail.com
7K8NDH	blackserpent34@gmail.com
8BHWAF	blackserpent34@gmail.com
8DP7RD	No lazystranger63 found. Only a lazystranger45.
9AEBRE	blackserpent34@gmail.com
9CPE9B	blackserpent34@gmail.com
A2MFXG	blackserpent34@gmail.com
AWRL2F	Not found.
AZRXWF	blackserpent34@gmail.com
B4BFFC	blackserpent34@gmail.com/"Lex Luther". (Cellebrite Extraction Report - Hangouts)
BX4PD7	In the comment he says his hangout account username is blackserpent34@gmail.com and this account name is also associated with the name Lex Luther.
C3CNWB	blackserpent34@gmail.com
C9GBYC	blackserpent34@gmail.com
D37Q26	blackserpent34@gmail.com
D8L2EA	blackserpent34@gmail.com
DHJ3QD	blackserpent34
DJFH4A	blackserpent34@gmail.com
DRKPJA	blackserpent34@gmail.com
E3HPVE	Lex Luther
EG36YD	blackserpent34@gmail.com
EMVHN9	Lex Luther, blackserpent34@gmail.com

TABLE 1

Question 17 - Applications

WebCode	Response
FWP664	blackserpent34@gmail.com
FXKN86	Lex luther
G63GVA	blackserpent34@gmail.com
GKUDX6	Hello, I bet you feel terrible! I have a sure way to get back at them. Add me on google hangout-blackserpent34@gmail.com. userdata (ExtX)/Root/data/com.tumblr/databases/Tumblr.sqlite
GNTPT6	blackserpent34@gmail.com
GQNYD8	blackserpent34@gmail.com Lex Luther
GRQTE7	blackserpent34@gmail.com
JZ4RHZ	blackserpent34@gmail.com
K7GAZZ	Lex Luther, blackserpent34@gmail.com
KGL8Y2	blackserpent34@gmail.com Lex Luthor
KJ6YQY	The lazystranger63's google hangout account username is: blackserpent34@gmail.com
KJNZ38	blackserpent34@gmail.com
KNHWRY	Blackserpent34@gmail.com
KUA4A8	I navigated to the Tumblr directory (data/com.tumblr), where I viewed all of the content within this folder. A Tumblr database file (tumblr.sqlite) was located inside of the shared_prefs folder (com.tumblr/shared_prefs/tumblr.sqlite), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, there was a message present that indicates that lazystranger63's Google Hangout account username is as follows: - blackserpant34@gmail.com
KZFX43	blackserpent34
L66WV3	Lex Luther
L6LTN3	blackserpent34@gmail.com
LYLK83	blackserpent34@gmail.com
M3ZEMY	blackserpent34@gmail.com
M9L8YY	Lex Luther
MDGY8V	blackserpent34@gmail.com
MHCT6X	blackserpent34@gmail.com
NDV89V	Blackserpent34@gmail.com
NGBFWV	blackserpent34@gmail.com
NUDXH3	Blackserpent34@gmail.com
PK8DUZ	Lex Luther
QCCWH2	blackserpent34@gmail.com
QQ8CHV	Lex Luther
QVK6NT	blackserpent34@gmail.com
RGCV7W	blackserpent34@gmail.com
RR6VHG	blackserpent34@gmail.com
T8QRYW	blackserpent34@gmail.com
TT8FBU	Did not recover "lazystranger63" account.

TABLE 1

Question 17 - Applications

WebCode	Response
UFLZ8U	Lex Luther. It is associated with the email address 'blackserpent34@gmail.com'.
UQC6QQ	blackserpent34@gmail.com
URBWAT	blackserpent34@gmail.com
V2AL8P	Lex Luther
VHGMPN	blackserpent34@gmail.com
VJC6QP	blackserpent34@gmail.com
VN3F2M	blackserpent34@gmail.com
WWD2MW	blackserpent34@gmail.com
XN3Y2V	Not found
YHLTAN	blackserpent34@gmail.com
ZKATLG	Could not determine
ZVTJVL	blackserpent34@gmail.com
ZWTAEN	No lazystranger63 found anywhere on this device. However there is a lazystranger45

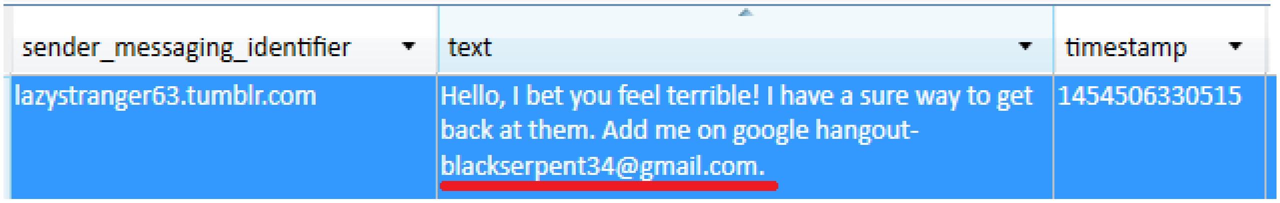
Consensus Result: blackserpent34@gmail.com

Expected Response Explanation:

Information about Tumblr messages can be found in the tumblr.sqlite database. The messaging_messages table will show the message containing the Google Hangout's username. The file can be found at:
data\com.tumblr\databases\tumblr.sqlite

Expected Response Illustration:

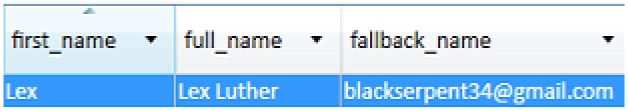
Database: tumblr.sqlite >>> Table: messaging_messages



sender_messaging_identifier	text	timestamp
lazystranger63.tumblr.com	Hello, I bet you feel terrible! I have a sure way to get back at them. Add me on google hangout-blackserpent34@gmail.com.	1454506330515

Other Responses:

Eight participants reported Lex Luther. These participants referred to the account owner of blackserpent34@gmail.com, Lex Luther. To determine Lex Luther these participants navigated outside of Tumblr to the the Babel1 database file within the com.google.android.talk folder and viewed the participant table. Lex Luther is identified along with his Google e-mail address blackserpent34@gmail.com. The file can be found at:
\data\com.google.android.talk\databases\babel1.db.
Database: babel1 >>> Table: participant



first_name	full_name	fallback_name
Lex	Lex Luther	blackserpent34@gmail.com

TABLE 1

Question 18 - Applications

Question 18: In Google maps a user requested driving directions to a park. Provide the full name of the park.

Manufacturer's Expected Response: Algonkian Regional Park

WebCode	Response
2EKP2R	Algonkian Regional Park
2L4XFF	Algonkian Regional Park
2T3MWK	Algonkian Regional Park
2ZYCPH	Algonkian Regional Park
3XNA9L	Algonkian Regional Park
4EAWZL	Algonkian Regional Park
67DGNM	Algonkian Regional Park – 47001 Fairway Dr. Sterling, VA 20165
6B4QXK	"Algonkian Regional Park"
6FZH7G	Algonkian Regional Park
6JJAHK	Algonkian Regional Park
6KETJL	Algonkian Regional Park
76HXLK	Algonkian Regional Park
77PFKG	Algonkian Regional Park
7BNU7K	Algonkian Regional Park
7K8NDH	Algonkian Regional Park
8BHWAF	Algonkian Regional Park
8DP7RD	Algonkian Regional Park
9AEBRE	Algonkian Park
9CPE9B	Algonkian Regional Park
A2MFXG	Algonkian Regional Park
AWRL2F	Algonkian Regional Park
AZRXWF	Algonkian Park
B4BFFC	Algonkian Regional Park. (MSAB Extraction Report - Locations/Bookmarks)
BX4PD7	Algonkian Regional Park Address provided: 47001 Fairway Dr, Sterling, VA 20165
C3CNWB	Algonkian Regional Park
C9GBYC	Algonkian Regional Park
D37Q26	Algonkian Regional Park
D8L2EA	Algonkian Regional Park
DHJ3QD	Algonkian Regional Park
DJFH4A	Algonkian Park
DRKPJA	Algonkian Regional Park
E3HPVE	Algonkian Regional Park
EG36YD	Algonkian Regional Park
EMVHN9	Algonkian Regional Park

TABLE 1

Question 18 - Applications

WebCode	Response
FWP664	Algonkian Regional Park
FXKN86	Algonkian Regional Park
G63GVA	Algonkian Regional Park
GKUDX6	Algonkian regional Park userdata (ExtX)/Root/data/com.google.android.apps.maps/databases/gmm_storage.db-journal
GNTPT6	Algonkian Regional Park
GQNYD8	Algonkian Regional Park
GRQTE7	Algonkian Regional Park loch Sugarland Run, Virginia
JZ4RHZ	Algonkian Regional Park
K7GAZZ	Algonkian Regional Park
KGL8Y2	Algonkian Park (An internet search of this park indicates it is called Algonkian Regional Park)
KJ6YQY	The full name of the park is: „Algonkian Regional Park”.
KJNZ38	Algonkian Regional Park
KNHWRY	Algonkian Regional Park
KUA4A8	I navigated to the Google Maps directory (data/com.google.android.apps.maps), where I viewed all of the content within this folder. A Google Maps database file (gmm_storage.db-journal) was located inside of the database folder (com.google.android.apps.maps/database/gmm_storage.db-journal), then viewed within EnCase 7 and it was determined that the name and address requested of the park is as follows: Algonkian Regional Park 47001 Fairway Drive Sterling, VA 20165
KZFX43	Algonkian Regional Park
L66WV3	Algonkian Regional Park
L6LTN3	Algonkian Regional Park
LYLK83	Algonkian Regional Park
M3ZEMY	Algonkian Regional Park
M9L8YY	Algonkian Park
MDGY8V	Algonkian Regional Park
MHCT6X	Algonkian Regional Park
NDV89V	Algonkian Regional Park
NGBFWV	Algonkian Regional Park
NUDXH3	Algonkian Regional Park
PK8DUZ	Algonkian Park
QCCWH2	Northern Virginia Regional Park Authority Algonkian Regional Park
QQ8CHV	Riverfront Cottages at Algonkian Regional Park
QVK6NT	Algonkian Regional Park
RGCV7W	Algonkian Regional Park
RR6VHG	Nortnen Virginia Regional Park Algonkian Regional Park
T8QRYW	Algonkian Regional Park
TT8FBU	Algonkian Regional Park
UFLZ8U	Algonkian Regional Park

TABLE 1

Question 18 - Applications

WebCode	Response
UQC6QQ	Algonkian Park
URBWAT	Algonkian Regional Park
V2AL8P	Algonkian Regional Park
VHGMPN	Algonkian Regional Park
VJC6QP	Algonkian Regional Park
VN3F2M	Algonkian Regional Park
WWD2MW	Algonkian Regional Park
XN3Y2V	Algonkian Regional Park
YHLTAN	Algonkian Regional Park 47001 Fairway Dr, Sterling, VA 20165
ZKATLG	Algonkian Park. From SMS messages.
ZVTJVL	Algonkian Regional Park
ZWTAEN	Algonkian Regional Park

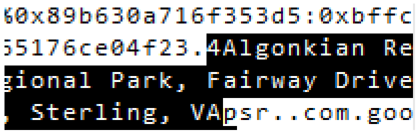
Consensus Result: Algonkian Regional Park

Expected Response Explanation:

Information about google map activity can be found in the gmm_storage.db data base. The sm_storage_table contains all the information about all of the activity on Google Maps. This file can be found at: \data\com.google.android.apps.maps\databases\gmm_storage.db

Expected Response Illustration:

Database: gmm_storage >>> Table: sm_storage_table



```
60x89b630a716f353d5:0xbffc
55176ce04f23.4Algonkian Re
gional Park, Fairway Drive
, Sterling, VApsr..com.goo
```

TABLE 1

Question 19 - Applications

Question 19: What terms did the suspect search for via Google search engine? (items only need to be listed once)

Manufacturer's Expected Response: TP-ing
Best Toilet Paper
Charmin Ultra Soft

WebCode	Response
2EKP2R	TP-ing Best toilet paper Charmin Ultra Soft
2L4XFF	Best Toilet Paper Charmin Ultra Soft TP-ing
2T3MWK	TP-ing Best Toilet Paper Charmin Ultra Soft
2ZYCPH	TP-ing, Best Toilet Paper, Charmin Ultra Soft
3XNA9L	TP-ing, Best Toilet Paper, Charmin Ultra Soft
4EAWZL	Charmin Ultra Soft Best Toilet Paper TP-ing yahoo mail
67DGNM	yahoo mail, TP-ing, Best Toilet Paper, Charmin Ultra Soft
6B4QXK	“TP-ing”, “Best Toilet Paper”, “Charmin Ultra Soft”
6FZH7G	yahoo mail, Charmin Ultra Soft, Best Toilet Paper and TP-ing.
6JJAHK	Charmin Ultra Soft Best Toilet Paper TP-ing
6KETJL	TP-ing Best Toilet Paper Charmin Ultra Soft
76HXLK	Best Toilet Paper Charmin Ultra Soft TP-ing
77PFKG	yahoo mail, TP-ing, Best Toilet Paper, Charming Ultra Soft
7BNU7K	yahoo mail Charmin Ultra Soft Best Toilet Paper TP-ing
7K8NDH	best toilet paper charmin ultra soft yahoo mail TP-ing
8BHWAF	yahoo mail TP-ing Best Toilet Paper Charmin Ultra Soft
8DP7RD	Charmin Ultra Soft,Best Toilet Paper,TP-ing
9AEBRE	Charmin Ultra Soft, Best Toilet Paper, TP-ing
9CPE9B	TP-ing Best Toilet Paper Charmin Ultra Soft
A2MFXG	TP-ing, Best Toilet Paper, Charmin Ultra Soft, yahoo mail
AWRL2F	yahoo mail Charmin Ultra Soft Best Toilet Paper TP-ing
AZRXWF	Yahoo Mail, Charmin Ultra Soft, Best Toilet Paper, TP-ing
B4BFFC	Charmin Ultra Soft; Best Toilet Paper; TP-ing. (Cellebrite Extraction Report - Searched Items (Chrome))
BX4PD7	Charmin Ultra Soft Best Toilet Paper TP-ing Yahoo mail
C3CNWB	TP-ing Best Toilet Paper Charmin Ultra Soft
C9GBYC	Charmin Ultra Soft Best Toilet Paper and TP-ing
D37Q26	TP-ing Best Toilet Paper Charmin Ultra Soft
D8L2EA	Best Toilet Paper TP-ing Charmin Ultra Soft Yahoo mail
DHJ3QD	yahoo mail TP-ing Best Toilet Paper Charmin Ultra Soft
DJFH4A	Charmin Ultra Soft, Best Toilet Paper, TP-ing
DRKPJA	TP-ing Best toilet paper Charmin Ultra Soft yahoo mail
E3HPVE	Best toilet paper
EG36YD	Yahoo mail, tumblr, Charmin Ultra Soft, Best Toilet Paper, TP-ing

TABLE 1

Question 19 - Applications

WebCode	Response
EMVHN9	Charmin Ultra Soft, Best Toilet Paper, and TP-ing.
FWP664	Charmin Ultra Soft, Best Toilet Paper, TP-ing, yahoo mail
FXKN86	"TP-ing", "Best Toilet Paper" and "Charmin Ultra soft"
G63GVA	yahoo mail, TPing, Best toilet paper, Charmin Ultra Soft,
GKUDX6	Tp-ing Best toilet paper Charmin ultra soft userdata (ExtX)/Root/data/com.android.chrome/app_chrome/Default/History
GNTPT6	TP-ing Best Toilet Paper Charmin Ultra Soft yahoo mail
GQNYD8	Charmin Ultra Soft Best Toilet Paper TP-ing
GRQTE7	1-TP-ing 2-Best Toilet Paper 3-Charmin Ultra Soft
JZ4RHZ	yahoo mail, TP-ing, Best Toilet Paper, and Charmin Ultra Soft
K7GAZZ	Charmin Ultra Soft, Best Toilet Paper, TP-ing, yahoo mail
KGL8Y2	tumblr Charmin Ultra Soft Best Toilet Paper TP-ing
KJ6YQY	tp-ing; best toilet paper; charmin ultra soft
KJNZ38	yahoo mail Best toilet paper Charmin ultra soft TP-ing
KNHWRY	Charmin Ultra Soft, Best Toilet Paper, TP-ing
KUA4A8	I navigated to the Android Browser directory (data/com.android.browser), where I viewed all of the content within this folder. A Browser database file (browser2.db) was located inside of the database folder (com.android.browser/database/browser2.db), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, there was evidence that the following terms were search using Google: - Yahoo Mail I navigated to the Android Chrome directory (data/com.android.chrome), where I viewed all of the content within this folder. A History file (History) was located inside of the default folder (com.android.chrome/default/History), then viewed within EnCase 7 and it was determined that the additional Google searches were conducted: - Best Toilet Paper - Charmin Ultra Soft
KZFX43	Charmin Ultra Soft, Best Toilet Paper, Tp-ing, yahoo.com
L66WV3	Charmin Ultra Soft Best Toilet Paper TP-ing
L6LTN3	TP-ing Best Toilet Paper Charmin Ultra Soft
LYLK83	yahoo mail, Charmin Ultra Soft, Best Toilet Paper, TP-ing
M3ZEMY	Best toilet paper TP-ing Charmin Ultra Soft
M9L8YY	Charmin Ultra Soft Best Toilet Paper TP-ing
MDGY8V	yahoo mail, Charmin Ultra Soft, Best Toilet Paper, TP-ing
MHCT6X	Charmin Ultra Soft, Best Toilet Paper, TP-ing , yahoo mail
NDV89V	Best Toilet Paper Charmin Ultra Soft TP-ing yahoo mail
NGBFWV	Charmin Ultra Soft, Best Toilet Paper, TP-ing
NUDXH3	Charmin Ultra Soft Best Toilet Paper TP-ing
PK8DUZ	TP-ing, Best Toilet Paper, Charmin Ultra Soft
QCCWH2	yahoo mail, Charmin Ultra Soft, Best Toilet Paper, TP-ing
QQ8CHV	yahoo mail, TP-ing, Best Toilet Paper, Charmin Ultra Soft
QVK6NT	yahoo mail, Charmin Ultra Soft, Best Toilet Paper, TP-ing
RGCV7W	Charmin Ultra Soft Best Toilet Paper TP-ing yahoo mail - search within Chrome Application

TABLE 1

Question 19 - Applications

WebCode	Response
RR6VHG	1-Charmen Ultra Soft 2- Best Toilet Paper 3- TP-ing
T8QRYW	Charmin Ultra Soft Best Toilet Paper TP-ing
TT8FBU	Best Toilet Paper,Charmin Ultra Soft, TP-ing
UFLZ8U	Charmin Ultra Soft, Best Toilet Paper, TP-ing
UQC6QQ	Charmin Ultra Soft, Best Toilet Paper, TP-ing
URBWAT	best toilet paper TP-ing Charmin Ultra Soft
V2AL8P	TP-ing Best Toilet Paper Charmin Ultra Soft
VHGMPN	Charmin Ultra Soft, Best Toilet Paper, TP-ing
VJC6QP	TP-ing Best Toilet Paper Charmin Ultra Soft
VN3F2M	Charmin Ultra Soft Best Toilet Paper TP-ing
WWD2MW	TP-ing Best Toilet Paper Charmin Ultra Soft
XN3Y2V	yahoo mail, TPing, Best toilet paper, Charmin ultra soft
YHLTAN	yahoo mail TP-ing Charmin Ultra Soft Best Toilet Paper
ZKATLG	Best Toilet Paper, TP-ing, Charmin Ultra Soft
ZVTJVL	Charmin Ultra Soft Best Toilet Paper TP-ing
ZWTAEN	best toilet paper Charmin Ultra Soft TP-ing

Consensus Result: TP-ing
Best Toilet Paper
Charmin Ultra Soft

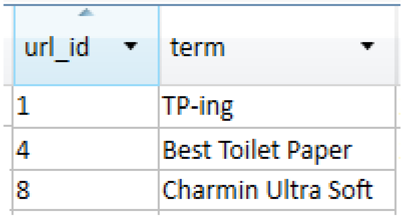
Expected Response Explanation:

Consensus was achieved for question 19. Information about the Google search engine can be found in the history database. The keyword_search_terms table will show the terms searched. The file can be found at:
\data\com.android.chrome\app_chrome\default\history

Additionally, 32 particiants discovered Yahoo Mail as a search term. These participants that reported Yahoo Mail within their response found the search term within the browser2 database of com.android.browser. The searches table displays the value searched. Information about the Yahoo Mail search term can be found at:
\data\com.android.browser\databases\browser2.db.

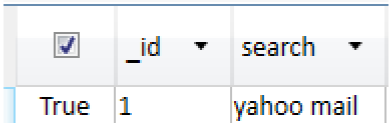
Expected Response Illustration:

Database: history >>> Table: keyword_search_terms



url_id	term
1	TP-ing
4	Best Toilet Paper
8	Charmin Ultra Soft

Database: browser2 >>> Table: searches



☑	_id	search
True	1	yahoo mail

TABLE 1

Question 20 - Applications

Question 20: What are the names of the downloaded items via Google Chrome?

<u>Manufacturer's Expected Response</u>: download.jpg
download(1).jpg

WebCode	Response
2EKP2R	download.jpg download(1).jpg
2L4XFF	download.jpg download(1).jpg
2T3MWK	download.jpg download(1).jpg
2ZYCPH	download.jpg, download(1).jpg
3XNA9L	/storage/emulated/0/Download/download.jpg , /storage/emulated/0/Download/download(1).jpg
4EAWZL	download.jpg download(1).jpg
67DGNM	download.jpg, download(1).jpg
6B4QXK	"download.jpg" and "download(1).jpg"
6FZH7G	download.jpg and download(1).jpg
6JJAHK	download.jpg download(1).jpg
6KETJL	download(1).jpg download.jpg
76HXLK	download.jpg download(1).jpg
77PFKG	download.jpg, download(1).jpg
7BNU7K	download.jpg download(1).jpg
7K8NDH	download.jpg download(1).jpg
8BHWAF	download.jpg download(1).jpg
8DP7RD	download.jpg,download(1).jpg
9AEBRE	download(1).jpg, download.jpg, download_20160203_101053.png
9CPE9B	download.jpg download(1).jpg
A2MFXG	download.jpg, download(1).jpg
AWRL2F	download.jpg download(1).jpg
AZRXWF	download.jpg download(1).jpg
B4BFFC	Two (2) items were downloaded via Google Chrome. The names of the two downloaded items were: "download.jpg" and "download(1).jpg". (downloads.db, Downloads table)
BX4PD7	download(1).jpg Download.jpg Download_20160203_101053.png
C3CNWB	download.jpg download(1).jpg
C9GBYC	download.jpg and download(1).jpg
D37Q26	download.jpg download(1).jpg
D8L2EA	download.jpg download(1).jpg
DHJ3QD	download.jpg download(1).jpg
DJFH4A	download.jpg and download(1).jpg
DRKPJA	download download(1) download_20160203_101053
E3HPVE	download.jpeg download(1).jpeg
EG36YD	download.jpg, download(1).jpg
EMVHN9	Two downloaded items named download and download(1).

TABLE 1

Question 20 - Applications

WebCode	Response
FWP664	download.jpg, download(1).jpg
FXKN86	"download.jpg" and "download(1).jpg"
G63GVA	download.jpg, download(1).jpg
GKUDX6	Download.jpg and download(1).jpg userdata (ExtX)/Root/data/com.android.chrome/app_chrome/Default/History
GNTPT6	download.jpg download(1).jpg
GQNYD8	download.jpg download(1).jpg
GRQTE7	1-download.jpg 2-download(1).jpg
JZ4RHZ	download.jpg and download(1).jpg
K7GAZZ	download.jpg, download(1).jpg
KGL8Y2	download.jpg download(1).jpg
KJ6YQY	download.jpg, download(1).jpg
KJNZ38	download.jpg download(1).jpg
KNHWRY	download.jpg, download(1).jpg
KUA4A8	I navigated to the download directory (data/media/0/download), where I viewed all of the content within this folder. A download database file (download.db) was located inside of the download folder (media/0/download/download.db), then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, there was evidence that the following files were downloaded: download.jpg download(1).jpg
KZFX43	download.jpg, download(1).jpg
L66WV3	download.jpg and download(1).jpg
L6LTN3	download.jpg download(1).jpg
LYLK83	download.jpg, download(1).jpg
M3ZEMY	download.jpg download(1).jpg
M9L8YY	download.jpg download(1).jpg
MDGY8V	download.jpg and download(1).jpg
MHCT6X	download.jpg, download(1).jpg
NDV89V	Download.jpg Download(1).jpg
NGBFWV	download.jpg, download(1).jpg
NUDXH3	Storage/emulated/0/Download/download.jpg storage/emulated/0/Download/download(1).jpg One is a picture of a house with paper on trees, the other is Charmin Ultra Soft.
PK8DUZ	downloadl.jpg, download(1).jpg
QCCWH2	download.jpg, download(1).jpg
QQ8CHV	download.jpg
QVK6NT	download.jpg download(1).jpg
RGCV7W	download.jpg download(1).jpg
RR6VHG	1-download.jpg 2-download(1).jpg
T8QRYW	download.jpg download(1).jpg
TT8FBU	download.jpg, download(1).jpg
UFLZ8U	'download.jpg' and 'download(1).jpg'

TABLE 1

Question 20 - Applications

WebCode	Response
UQC6QQ	download.jpg and download(1).jpg
URBWAT	download.jpg download(1).jpg
V2AL8P	download.jpg download(1).jpg
VHGMPN	download.jpg, download(1).jpg
VJC6QP	download.jpg download(1).jpg
VN3F2M	download.jpg download(1).jpg
WWD2MW	download.jpg download.jpg (1)
XN3Y2V	download.jpg download(1).jpg
YHLTAN	download(1).jpg download.jpg
ZKATLG	download(1).jpg Download.jpg Download_20160203_101053.png 140 pictures of toilet paper in android.chrome.cache
ZVTJVL	download.jpg download(1).jpg
ZWTAEN	download.jpg download(1).jpg

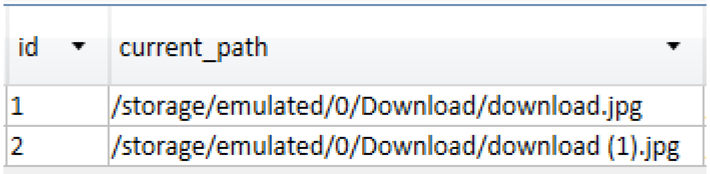
Consensus Result: download.jpg and download(1).jpg

Expected Response Explanation:

Information about the Google Chrome downloaded files can be found in the history database. The downloads table will show downloaded files from Chrome. The file can be found at: data\com.android.chrome\app_chrome\default\history

Expected Response Illustration:

Database: history >>> Table: downloads



id	current_path
1	/storage/emulated/0/Download/download.jpg
2	/storage/emulated/0/Download/download (1).jpg

TABLE 1

Question 21 - Applications

Question 21: Via Instagram a picture of a suspension slip was posted. What is the student ID # on the slip?

Manufacturer's Expected Response: 190199

WebCode	Response
2EKP2R	190199
2L4XFF	Student ID: 190199
2T3MWK	190199
2ZYCPH	190199
3XNA9L	190199
4EAWZL	190199
67DGNM	Student id: 190199
6B4QXK	190199
6FZH7G	190199
6JJAHK	190199
6KETJL	190199
76HXLK	190199
77PFKG	190199
7BNU7K	190199
7K8NDH	190199
8BHWAF	190199
8DP7RD	190199
9AEBRE	190199
9CPE9B	190199
A2MFXG	190199
AWRL2F	190199
AZRXWF	190199
B4BFFC	190199. (Cellebrite Extraction Report - Images)
BX4PD7	Student ID: 190199
C3CNWB	190199
C9GBYC	190199
D37Q26	190199
D8L2EA	190199
DHJ3QD	190199
DJFH4A	190199
DRKPJA	190199
E3HPVE	190199
EG36YD	190199
EMVHN9	190199
FWP664	Student ID:190199

TABLE 1

Question 21 - Applications

WebCode	Response
FXKN86	190199
G63GVA	190199
GKUDX6	St3llar8 ID 2307817547 userdata (ExtX)/Root/data/com.instagram.android/app_webview/Cookies
GNTPT6	190199
GQNYD8	190199
GRQTE7	190199
JZ4RHZ	190199
K7GAZZ	ID:190199
KGL8Y2	190199
KJ6YQY	Student Id# is: 190199
KJNZ38	190199
KNHWRY	190199
KUA4A8	There are a number of ways to obtain this information, but I located a picture of the suspension slip extracted from the cellular device forensic image using Internet Evidence Finder (IEF). The IEF picture indicates that the student ID number is as follows: - 190199
KZFX43	190199
L66WV3	190199
L6LTN3	190199
LYLK83	190199
M3ZEMY	190199
M9L8YY	190199
MDGY8V	190199
MHCT6X	190199
NDV89V	190199
NGBFWV	190199
NUDXH3	Stella Frost ID 190199
PK8DUZ	190199
QCCWH2	190199
QQ8CHV	190199
QVK6NT	190199
RGCV7W	190199
RR6VHG	190199
T8QRYW	190199
TT8FBU	190199
UFLZ8U	190199
UQC6QQ	190199
URBWAT	190199
V2AL8P	190199

TABLE 1

Question 21 - Applications

WebCode	Response
VHGMPN	190199
VJC6QP	190199
VN3F2M	190199
WWD2MW	190199
XN3Y2V	190199
YHLTAN	190199
ZKATLG	190199
ZVTJVL	190199
ZWTAEN	190199

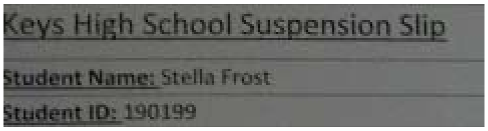
Consensus Result: 190199

Expected Response Explanation:

The Instagram images can be viewed in the following location:
\media\0\Pictures\Instagram.

Expected Response Illustration:

Suspension Slip:

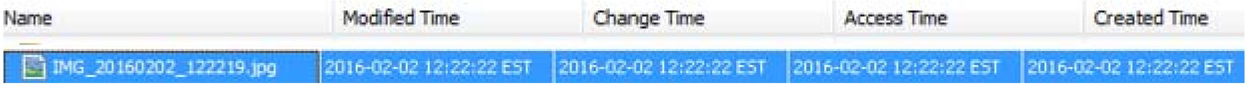


Keys High School Suspension Slip

Student Name: Stella Frost

Student ID: 190199

Instagram File Location:



Name	Modified Time	Change Time	Access Time	Created Time
IMG_20160202_122219.jpg	2016-02-02 12:22:22 EST	2016-02-02 12:22:22 EST	2016-02-02 12:22:22 EST	2016-02-02 12:22:22 EST

TABLE 1

Question 22 - Applications

Question 22: What is the name of the attachment that is sent via google hangouts?

Manufacturer's Expected Response: DIY_Toilet%2BPaper.PNG

WebCode	Response
2EKP2R	DIY_Toilet Paper.png
2L4XFF	DIY_Toilet Paper.PNG
2T3MWK	DIY_Toilet%2BPaper.PNG
2ZYCPH	DIY_ToiletPaper.png
3XNA9L	DIY_Toilet%2BPaper.PNG
4EAWZL	DIY_Toilet Paper.PNG
67DGNM	DIY_Toilet%2BPaper.PNG
6B4QXK	“DIY_Toilet Paper.PNG”
6FZH7G	DIY_Toilet Paper.PNG
6JJAHK	DIY_Toilet Paper.PNG
6KETJL	DIY_Toilet%2BPaper.PNG
76HXLK	DIY_Toilet%2BPaper.PNG
77PFKG	DIY_Toilet Paper.png
7BNU7K	DIY_Toilet Paper.PNG
7K8NDH	DIY_Toilet Paper.PNG
8BHWAF	DIY_Toilet%2BPaper.PNG
8DP7RD	DIY_Toilet Paper.PNG
9AEBRE	DIY_Toilet Paper.PNG
9CPE9B	DIY_Toilet Paper.PNG
A2MFXG	DIY_Toilet%2BPaper.PNG
AWRL2F	DIY Toilet Paper.PNG
AZRXWF	DIY_Toilet Paper.PNG
B4BFFC	DIY_Toilet Paper.PNG. (Cellebrite Extraction Report - Chats)
BX4PD7	DIY_Toilet Paper
C3CNWB	https://lh3.googleusercontent.com/-19C3b8kCbUY/VrIYYfcPdaI/AAAAAAAABU/Li7sQm6biO8/s0/DIY_Toilet%2BPaper.PNG
C9GBYC	DIY_Toilet Paper.PNG
D37Q26	DIY_Toilet Paper.PNG
D8L2EA	DIY_Toilet Paper.PNG
DHJ3QD	DIY Toilet Paper.PNG
DJFH4A	DIY_Toilet Paper.PNG
DRKPJA	DIY_toilet%2bpaper
E3HPVE	DIY_Toilet Paper.PNG
EG36YD	DIY_Toilet%2BPaper.PNG
EMVHN9	DIY_ToiletPaper.PNG

TABLE 1

Question 22 - Applications

WebCode	Response
FWP664	https://lh3.googleusercontent.com/-19C3b8kCbUY/VrIYYfcPdaI/AAAAAAAAABU/Li7sQm6biO8/s0/DIY_Toilet%2BPaper.PNG
FXKN86	DIY_Toilet%2BPaper.PNG
G63GVA	DIY_ToiletPaper.png
GKUDX6	DIY_Toilet Paper.png userdata (ExtX)/Root/data/com.google.android.talk/cache/volleyCache/1434410069.0/DIY_Toilet Paper.PNG" userdata (ExtX)/Root/data/com.google.android.talk/databases/babel1.db
GNTPT6	DIY_Toilet%2BPaper.PNG
GQNYD8	DIY_Toilet Paper.PNG
GRQTE7	DIY_Toilet%2BPaper.PNG
JZ4RHZ	DIY_Toilet Paper.PNG
K7GAZZ	DIY_Toilet+Paper.PNG
KGL8Y2	DIY_Toilet Paper.PNG
KJ6YQY	Name of attachment is „DIY_Toilet%2BPaper.PNG”. full pach is https://lh3.googleusercontent.com/-19C3b8kCbUY/VrIYYfcPdaI/AAAAAAAAABU/Li7sQm6biO8/s0/DIY_Toilet%2BPaper.PNG
KJNZ38	DIY_Toilet Paper.png
KNHWRY	DIY_Toilet Paper.PNG
KUA4A8	There are a number of ways to obtain this information, but I located and analyzed the pictures extracted from the cellular device forensic image using Internet Evidence Finder (IEF). The IEF picture indicates that the attachments sent via Google Hangouts are as follows: Falling_Stella.jpg Falling_Stella-1.jpg
KZFX43	DIY_Toilet Paper.png
L66WV3	DIY Toilet Paper.PNG
L6LTN3	DIY_Toilet Paper.PNG
LYLK83	DIY_Toilet%2BPaper.PNG
M3ZEMY	DIY_Toilet Paper.PNG "Making Your Own Toilet Paper"
M9L8YY	DIY_Toilet Paper.PNG
MDGY8V	DIY_Toilet Paper.png
MHCT6X	DIY_Toilet Paper.PNG
NDV89V	DIY_Toilet Paper.png
NGBFWV	DIY_Toilet%2BPaper.PNG
NUDXH3	DIY_Toilet Paper.PNG
PK8DUZ	DIY_Toilet Paper.PNG
QCCWH2	DIY_Toilet%2BPaper.PNG
QQ8CHV	DIY_Toilet Paper.PNG
QVK6NT	DIY_Toilet Paper.PNG
RGCV7W	DIY_Toiletpaper.png
RR6VHG	DIY_Toilet Paper.PNG
T8QRYW	DIY_Toilet Paper.png

TABLE 1

Question 22 - Applications

WebCode	Response
TT8FBU	DIY_Toilet Paper.PNG
UFLZ8U	DIY_Toilet Paper.PNG
UQC6QQ	DIY_Toilet Paper.PNG
URBWAT	DIY_Toilet Paper.png
V2AL8P	DIY_Toilet Paper.PNG
VHGMPN	DIY_Toilet Paper.PNG
VJC6QP	DIY_Toilet Paper.PNG
VN3F2M	DIY_Toilet Paper.PNG
WWD2MW	DIY Toilet Paper.PNG
XN3Y2V	DIY Toilet Paper.png
YHLTAN	DIY_Toilet Paper.PNG
ZKATLG	DIY_Toilet Paper.png
ZVTJVL	https://lh3.googleusercontent.com/-19C3b8kCbUY/VrIYYfcPdaI/AAAAAAAAABU/Li7sQm6biO8/s0/DIY_Toilet%2BPaper.PNG
ZWTAEN	DIY-Toilet Paper.png

Consensus Result: DIY_Toilet Paper.PNG

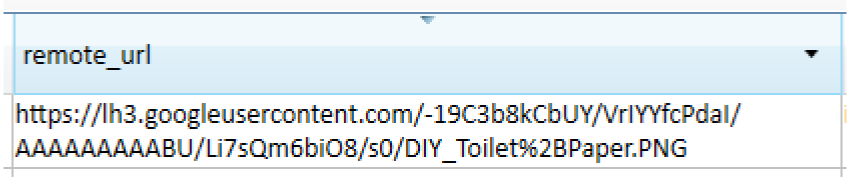
Expected Response Explanation:

Information about attachments sent via Google Hangouts can be seen in the babel1.db database. The messages table shows information on attachments exchanged. The file can be found at:
\data\com.google.android.talk\databases\babel1.db

Differences in responses regarding the reporting of a space or "%2B" is believed to be due to the tool utilized for examination.

Expected Response Illustration:

Database: babel1 >>> Table: messages



remote_url
https://lh3.googleusercontent.com/-19C3b8kCbUY/VrIYYfcPdaI/AAAAAAAAABU/Li7sQm6biO8/s0/DIY_Toilet%2BPaper.PNG

TABLE 1

Question 23 - Applications

Question 23: Which third-party application was the last to be downloaded on Friday, January 22, 2016? (ANSWERS MUST HAVE BOTH THE "package_name" and "title")

Manufacturer's Expected Response: Package_name: "com.facebook.orca"
Title: "Messenger"

WebCode	Response
2EKP2R	Facebook Messenger com.facebook.orca
2L4XFF	Messenger com.facebook.orca
2T3MWK	Package_name: com.facebook.orca Title: Facebook Messenger
2ZYCPH	"com.facebook.katana" "Facebook"
3XNA9L	com.lge.qmemoplus, Quick Memo
4EAWZL	com.facebook.orca Messenger
67DGNM	package_name:com.facebook.orca Title: Messenger
6B4QXK	"com.facebook.orca" and "Messenger"
6FZH7G	com.facebook.orca Messenger
6JJAHK	package_name: com.facebook.orca title: Messenger
6KETJL	Package Name= com.facebook.orca Title: Messenger
76HXLK	com.facebook.orca = Messenger
77PFKG	com.facebook.orca / Messenger
7BNU7K	com.facebook.orca Messenger
7K8NDH	(com.facebook.orca) Facebook Messenger
8BHWAF	com.facebook.orca Messenger
8DP7RD	Facebook Messenger com.facebook.orca
9AEBRE	com.facebook.orca, Messenger
9CPE9B	com.facebook.orca Facebook Messenger
A2MFXG	com.facebook.orca, Messenger
AWRL2F	com.facebook.orca Messenger
AZRXWF	com.facebook.orca Facebook Messenger
B4BFFC	package_name: com.facebook.orca, title: Messenger. (localappstate.db, Appstate table, and Cellebrite Extraction Report - Installed Applications)
BX4PD7	Com.facebook.orca and Messenger was the last app to be installed on January 22, 2016 at 12:45:27 PM (UTC-5) according to the timeline.
C3CNWB	package_name : com.facebook.orca title : Messenger
C9GBYC	package_name: com.facebook.orca title: Messenger
D37Q26	package_name com.facebook.orca title Messenger
D8L2EA	Facebook Messenger Package Name: com.facebook.orca
DHJ3QD	com.facebook.orca Messenger
DJFH4A	com.facebook.orca Messenger
DRKPJA	com.facebook.orce Messenger
E3HPVE	"package_name" = com.skype.raider "title" = Skype-free IM & video calls
EG36YD	com.facebook.orca, Messenger

TABLE 1

Question 23 - Applications

WebCode	Response
EMVHN9	Com.facebook.orca, Messenger
FWP664	com.facebook.orca, Messenger
FXKN86	Package name: "com.facebook.orca" and Title "Facebook Messenger"
G63GVA	Package_name=com.facebook.orca title=Messenger
GKUDX6	Com.facebook.orca package name Messenger title userdata (ExtX)/Root/data/com.android.vending/databases/localappstate.db
GNTPT6	com.facebook.orca Facebook Messenger
GQNYD8	com.facebook.orca Messenger package_name: com.facebook.orca title: Messenger
GRQTE7	1- Tumblr / com.tumblr 2- Skype for Business / com.microsoft.office.lync15 3- Skype / com.skype.raider 4- Instagram / com.instagram.android 5- Facebook / com.facebook.katana 6- Messenger / com.facebook.orca
JZ4RHZ	com.facebook.orca, Messenger
K7GAZZ	"com.facebook.orca-1\base.apk" "Messenger"
KGL8Y2	"package_name" com.facebook.orca "title" Messenger
KJ6YQY	package_name:”com.facebook.orca” and title: ”Messenger”.
KJNZ38	com.facebook.orca Messenger
KNHWRY	com.facebook.orca Messenger
KUA4A8	Based on the analysis of the installed third-party applications, it was determined that Facebook was the last to be downloaded on the device. The following is the answer in the required format: "package_name" = com.facebook.orca Facebook Messenger (Orca)
KZFX43	package name: com.facebook.orca Facebook Messenger
L66WV3	com.facebook.orca Messenger
L6LTN3	Messenger com.facebook.orca
LYLK83	com.facebook.orca / Messenger
M3ZEMY	com.facebook.orca Messenger
M9L8YY	com.facebook.orca Messenger
MDGY8V	package name: com.facebook.orca Title Facebook.
MHCT6X	DIY_Toilet Paper.PNG
NDV89V	com.facebook.orca Messenger
NGBFWV	package_name: com.facebook.orca title: Messenger
NUDXH3	com.facebook.orca (messenger)
PK8DUZ	android-1/base.apk/Android Manifest.xml instagram
QCCWH2	"data@app@com.facebook.orca-1@base.apk@classes.dec" "Messenger"
QQ8CHV	com.facebook.orca, Messenger
QVK6NT	Com.facebook.orca Messenger
RGCV7W	Messenger, com.Facebook.orca
RR6VHG	1-com.facebook.orca 2-Messenger
T8QRYW	Package_name = “base.apk” Title is “Messenger”
TT8FBU	Facebook Messenger com.facebook.orca

TABLE 1

Question 23 - Applications

WebCode	Response
UFLZ8U	“package_name” is com.facebook.orca. "title" is Messenger.
UQC6QQ	com.facebook.orca Messenger
URBWAT	Package Name: com.facebook.orca Title: Messenger
V2AL8P	package_name = com.facebook.orca title = Messenger
VHGMPN	“com.facebook.orca” & “Messenger”
VJC6QP	com.facebook.orca Messenger
VN3F2M	Com.facebook.orca Messenger
WWD2MW	Facebook Messenger com.facebook.orca
XN3Y2V	com.facebook.orca messenger
YHLTAN	com.facebook.orca "Messenger"
ZKATLG	Com.facebook.orca-1, Messenger
ZVTJVL	package_name: com.facebook.orca title: Messenger
ZWTAEN	Messenger com.facebook.orca

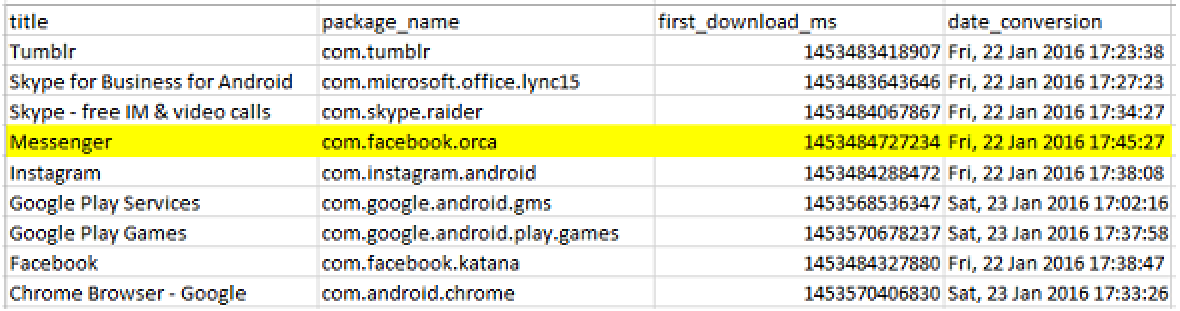
Consensus Result: com.facebook.orca (Messenger)

Expected Response Explanation:

Information about the downloaded applications can be seen in the localappstate.db database. The localappstate.db database can be found at:
\data\com.android.vending\databases\localappstate.db

Expected Response Illustration:

Database: localappstate >>> Table: appstate



title	package_name	first_download_ms	date_conversion
Tumblr	com.tumblr	1453483418907	Fri, 22 Jan 2016 17:23:38
Skype for Business for Android	com.microsoft.office.lync15	1453483643646	Fri, 22 Jan 2016 17:27:23
Skype - free IM & video calls	com.skype.raider	1453484067867	Fri, 22 Jan 2016 17:34:27
Messenger	com.facebook.orca	1453484727234	Fri, 22 Jan 2016 17:45:27
Instagram	com.instagram.android	1453484288472	Fri, 22 Jan 2016 17:38:08
Google Play Services	com.google.android.gms	1453568536347	Sat, 23 Jan 2016 17:02:16
Google Play Games	com.google.android.play.games	1453570678237	Sat, 23 Jan 2016 17:37:58
Facebook	com.facebook.katana	1453484327880	Fri, 22 Jan 2016 17:38:47
Chrome Browser - Google	com.android.chrome	1453570406830	Sat, 23 Jan 2016 17:33:26

TABLE 1

Question 24 - Applications

Question 24: What is the body of the first message received via Skype from user Diane Chambers?

Manufacturer's Expected Response: Heard you failed the test! Serves you right dumb girl.

WebCode	Response
2EKP2R	"Heard you failed the test! Serves you right dumb girl."
2L4XFF	Heard you failed the test! Serves you right dumb girl.
2T3MWK	Heard you failed the test! Serves you right dumb girl.
2ZYCPH	Heard you failed the test! Serves you right dumb girl.
3XNA9L	cheerydear67
4EAWZL	Heard you failed the test! Serves you right dumb girl.
67DGNM	Heard you failed the test! Serves you right dumb girl.
6B4QXK	“Heard you failed the test! Serves you right dumb girl.”
6FZH7G	Heard you failed the test! Serves you right dumb girl.
6JJAHK	Heard you failed the test! Serves you right dumb girl.
6KETJL	Heard you failed the test! Serves you right dumb girl.
76HXLK	Heard you failed the test! Serves you right dumb girl.
77PFKG	Heard you failed the test! Serves you right dumb girl.
7BNU7K	Heard you failed the test! Serves you right dumb girl.
7K8NDH	Heard you failed the test! Serves you right dumb girl.
8BHWAF	Heard you failed the test! Serves you right dumb girl.
8DP7RD	Heard you failed the test! Serves you right dumb girl.
9AEBRE	Heard you failed the test! Serves you right dumb girl.
9CPE9B	Heard yoy failed the test! Serves you right dumb girl.
A2MFXG	Heard you failed the test! Serves you right dumb girl.
AWRL2F	Heard you failed the test! Serves you right dumb girl.
AZRXWF	Heard you failed the test! Serves you right dumb girl.
B4BFFC	Heard you failed the test! Serves you right dumb girl. (Cellebrite Extraction Report - Chats)
BX4PD7	Heard you failed the test! Serves you right dumb girl.
C3CNWB	Heard you failed the test! Serves you right dumb girl
C9GBYC	Heard you failed the test! Serves you right dumb girl.
D37Q26	Heard you failed the test! Serves you right dumb girl.
D8L2EA	Heard you failed the test! Serves you right dumb girl.
DHJ3QD	Heard you failed the test! Serves you right dumb girl.
DJFH4A	Heard you failed the test! Serves you right dumb girl.
DRKPJA	Stella, you are dumb! Please stop coming to school!!!
E3HPVE	Heard you failed the test! Serves you right dumb girl.
EG36YD	Heard you failed the test! Serves you right dumb girl.
EMVHN9	“Heard you failed the test! Serves you right dumb girl.”
FWP664	Heard you failed the test! Serves you right dumb girl.

TABLE 1

Question 24 - Applications

WebCode	Response
FXKN86	Heard you failed the test! Serves you right dumb girl.
G63GVA	cheerydear67 02/01/2016 04:07:01PM
GKUDX6	Heard you failed the test! Serves you right dumb girl. userdata (ExtX)/Root/data/com.skype.raider/files/frosty.queen12/main.db
GNTPT6	Heard you failed the test! Serves you right dumb girl.
GQNYD8	"Heard you failed the test! Serves you right dumb girl."
GRQTE7	Heard you failed the test! Serves you right dumb girl
JZ4RHZ	Heard you failed the test! Serves you right dumb girl.
K7GAZZ	Heard you failed the test! Serves you right dumb girl.
KGL8Y2	Heard you failed the test! Serves you right dumb girl.
KJ6YQY	The body of the first message received via Skype from user Diane Chambers was: "Heard you failed the test! Serves you right dumb girl."
KJNZ38	Heard you failed the test! Serves you right dumb girl
KNHWRY	Heard you failed the test! Serves you right dumb girl.
KUA4A8	I navigated to the Skype directory (com.skype.raider) and exported the profile folder (frosty.queen12). The profile folder was opened with the SkypeLogView application, which generated the skype conversations. The body of the first message received via skype from Diane Chambers was as follows: - Heard you failed the test! Serves you right dumb girl. - cheerydear67 (Skype Username) - 02/02/2016 9:00:05AM - cheerydear67
KZFX43	Heard you failed the test! Serves you right dumb girl.
L66WV3	Heard you failed the test! Serves you right dumb girl.
L6LTN3	Heard you failed the test! Serves you right dumb girl.
LYLK83	Heard you failed the test! Serves you right dumb girl.
M3ZEMY	Heard you Failed the test! Serves you right dumb girl.
M9L8YY	Heard you failed the test! Serves you right dumb girl.
MDGY8V	Heard you failed the test! Serves you right dumb girl.
MHCT6X	Heard you failed the test! Serves you right dumb girl.
NDV89V	Heard you failed the test! Serves you right dumb girl.
NGBFWV	Heard you failed the test! Serves you right dumb girl.
NUDXH3	CheeryDear67- Heard you failed the test! Serves you right dumb girl!
PK8DUZ	Have yo failed the test! Serves you right dumb girl.
QCCWH2	Heard you failed the test! Serves you right dumb girl.
QQ8CHV	Heard you failed the test! Serves you right dumb girl.
QVK6NT	Heard you failed the test! Serves you right dumb girl.
RGCV7W	Heard you failed the test! Serves you right dumb girl!
RR6VHG	Heard you failed the test! Serves you right dumb girl.
T8QRYW	Heard you failed the test! Serves you right dumb girl.
TT8FBU	Heard you failed the test! Serves you right dumb girl.
UFLZ8U	Heard you failed the test! Serves you right dumb girl.
UQC6QQ	Heard you failed the test! Serves you right dumb girl.

TABLE 1

Question 24 - Applications

WebCode	Response
URBWAT	Heard you failed that test! Serves you right dumb girl.
V2AL8P	Heard you failed the test! Serves you right dumb girl.
VHGMPN	Heard you failed the test! Serves you right dumb girl.
VJC6QP	Heard you failed the test! Serves you right dumb girl.
VN3F2M	Heard you failed the test! Serves you right dumb girl.
WWD2MW	Heard you failed the test! Serves you right dumb girl.
XN3Y2V	"heard you failed the test! Serves you right dumb girl."
YHLTAN	cheerydear67
ZKATLG	Heard you failed the test! Serves you right dumb girl.
ZVTJVL	Heard you failed the test! Serves you right dumb girl. lisa frank
ZWTAEN	Heard you failed the test! Serves you right dumb girl.

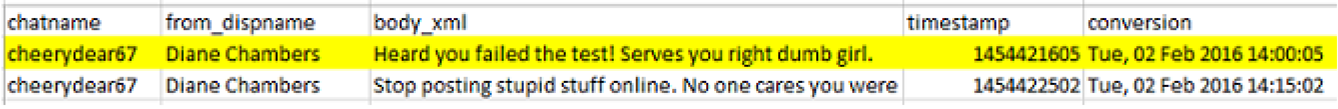
Consensus Result: Heard you failed the test! Serves you right dumb girl.

Expected Response Explanation:

Information about messages in Skype can be found in the main.db database. The messages table shows messages exchanged via Skype. To determine when the first message from Diane Chambers was sent the value in the timestamp column needs to be converted from Unix Epoch. The file can be found at:
\data\com.skype.raider\files\frosty.queen12\main.db.

Expected Response Illustration:

Database: main >>> Table: messages



chatname	from_dispname	body_xml	timestamp	conversion
cheerydear67	Diane Chambers	Heard you failed the test! Serves you right dumb girl.	1454421605	Tue, 02 Feb 2016 14:00:05
cheerydear67	Diane Chambers	Stop posting stupid stuff online. No one cares you were	1454422502	Tue, 02 Feb 2016 14:15:02

TABLE 1

Question 25 - Communications

Question 25: Please list the display name associated for the following contact number- 7039402942

Manufacturer's Expected Response: Lisa Frank

WebCode	Response
2EKP2R	Lisa Frank
2L4XFF	Lisa Frank
2T3MWK	Lisa Frank
2ZYCPH	Lisa Frank
3XNA9L	Lisa Frank
4EAWZL	Lisa Frank
67DGNM	Lisa Frank
6B4QXK	Lisa Frank
6FZH7G	Lisa Frank
6JJAHK	Lisa Frank
6KETJL	Lisa Frank
76HXLK	Lisa Frank
77PFKG	Lisa Frank
7BNU7K	Lisa Frank
7K8NDH	Lisa Frank
8BHWAF	Lisa Frank
8DP7RD	Lisa Frank
9AEBRE	Lisa Frank
9CPE9B	Lisa Frank
A2MFXG	Lisa Frank
AWRL2F	LISA FRANK
AZRXWF	Lisa Frank
B4BFFC	Lisa Frank. (Cellebrite Extraction Report - Contacts)
BX4PD7	Lisa Frank
C3CNWB	Lisa Frank
C9GBYC	Lisa Frank
D37Q26	Lisa Frank
D8L2EA	Lisa Frank
DHJ3QD	Lisa Frank
DJFH4A	Lisa Frank
DRKPJA	Lisa Frank
E3HPVE	Lisa Frank
EG36YD	Lisa Frank
EMVHN9	Lisa Frank
FWP664	Lisa Frank

TABLE 1

Question 25 - Communications

WebCode	Response
FXKN86	Lisa Frank
G63GVA	Lisa Frank
GKUDX6	Lisa Frank userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db
GNTPT6	Lisa Frank
GQNYD8	Lisa Frank
GRQTE7	Lisa Frank
JZ4RHZ	Lisa Frank
K7GAZZ	Lisa Frank
KGL8Y2	Lisa Frank
KJ6YQY	Frank Lisa
KJNZ38	Lisa Frank
KNHWRY	Lisa Frank
KUA4A8	The contacts2.db file was located, then exported to the target drive and viewed with SQLiteBrowser software. Based on the analysis of this data in the SQLiteBrowser application, it is determined that the display name associated with the 7039402942 contact number is as follows: - frankie.lis88 (Skype Username)
KZFX43	Lisa Frank
L66WV3	Lisa Frank
L6LTN3	Lisa Frank
LYLK83	Lisa Frank
M3ZEMY	Lisa Frank
M9L8YY	Lisa Frank
MDGY8V	Lisa Frank
MHCT6X	Lisa Frank
NDV89V	Lisa Frank
NGBFWV	Lisa Frank
NUDXH3	Lisa Frank
PK8DUZ	Lisa Frank
QCCWH2	Lisa Frank
QQ8CHV	Lisa Frank
QVK6NT	Lisa Frank
RGCV7W	Lisa Frank
RR6VHG	Lisa Frank
T8QRYW	Lisa Frank
TT8FBU	Lisa Frank
UFLZ8U	Lisa Frank
UQC6QQ	Lisa Frank
URBWAT	Lisa Frank

TABLE 1

Question 25 - Communications

WebCode	Response
V2AL8P	Lisa Frank
VHGMPN	Lisa Frank
VJC6QP	Lisa Frank
VN3F2M	Lisa Frank
WWD2MW	Lisa Frank
XN3Y2V	Lisa Frank
YHLTAN	Lisa Frank
ZKATLG	Lisa Frank
ZVTJVL	lisa frank
ZWTAEN	Lisa Frank

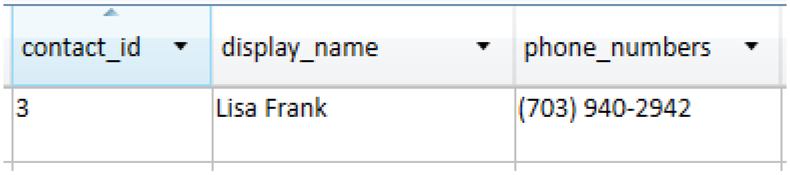
Consensus Result: Lisa Frank

Expected Response Explanation:

Information on the phone contact list can be found in the icingcorpora.db database. The contacts table shows contact information stored on this device. The icingcorpora.db database can be found at:
\data\com.google.android.googlequicksearchbox\databases\icingcorpora.db

Expected Response Illustration:

Database: icingcorpora >>> Table: contacts



contact_id	display_name	phone_numbers
3	Lisa Frank	(703) 940-2942

TABLE 1

Question 26 - Communications

Question 26: What phone number is associated with the following user names: LazyStranger63, blackserpent34, and LazyStranger45?

Manufacturer's Expected Response: 571-645-9269

WebCode	Response
2EKP2R	571-645-9269
2L4XFF	571-645-9269
2T3MWK	The user names points to the same person (Mr. Black) with phone number 571-645-9269
2ZYCPH	571-645-9269
3XNA9L	571-645-9269
4EAWZL	(571) 645-9269
67DGNM	571-645-9269
6B4QXK	+15716459269
6FZH7G	571-645-9269
6JJAHK	(571) 645-9269
6KETJL	(571) 645-9269
76HXLK	LazyStranger63, blackserpent34, and LazyStranger45 appear to be the same person Mr. Black who's phone number is 571-645-9269
77PFKG	571-645-9269
7BNU7K	571-645-9269
7K8NDH	(571) 645-9269
8BHWAF	571-645-9269
8DP7RD	blackserpent34-5716459269 lazystranger45-5716459269 lazystranger63-not recovered.
9AEBRE	571-645-9269
9CPE9B	(571)6459269
A2MFXG	(571) 645-9269
AWRL2F	(571) 645-9269
AZRXWF	571-645-9269 For All users.
B4BFFC	571-645-9269. (MSAB XRY Extraction Report - Contacts and Messages/Chats)
BX4PD7	571-645-9269
C3CNWB	571-645-9269
C9GBYC	571-645-9269
D37Q26	5716459269
D8L2EA	(571) 645-9269
DHJ3QD	571-645-9269
DJFH4A	(571) 645-9269
DRKPJA	571-645-9269
E3HPVE	(571)-645-9269
EG36YD	(571) 645-9269
EMVHN9	(571) 645-9269

TABLE 1

Question 26 - Communications

WebCode	Response
FWP664	(571)645-9269
FXKN86	Mobile: (571) 645-9269
G63GVA	LazyStranger63 is a tumblr account blackserpent34 is Lex Luther LazyStrange45 the Skype account of Blackserpent34, in contacts Mr. Black is listed as LazyStranger45, Mr. Black also has a contact with the phone number (571)645-9269. This number was provided in a chat by Mr. Black.
GKUDX6	Blackserpent34, LazyStranger63 and LazyStranger45 are Mr.Black 5716459269 userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db userdata (ExtX)/Root/data/com.skype.raider/files/frosty.queen12/main.db
GNTPT6	(571) 645-9269
GQNYD8	(571) 645-9269
GRQTE7	LazyStranger63 / LazyStranger45 / blackserpent34 = 571645-9269
JZ4RHZ	(571) 645-9269
K7GAZZ	5716459269
KGL8Y2	571-645-9269
KJ6YQY	Phone number: (571) 645-9269
KJNZ38	571-645-9269
KNHWRY	(571)645-9269
KUA4A8	The contacts2.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase software. Based on the analysis of this data, it is determined that the phone numbers associated with previously mentioned usernames are as follows: - LazyStranger45 - 571-645-9269 (Mr. Black) - LazyStranger63 - 145-450-6330 (Lex Luther) - blackserpent34 - 145-450-6330 (Lex Luther)
KZFX43	(571)645-9269
L66WV3	(571) 645-9269
L6LTN3	(571)645-9269
LYLK83	(571)645-9269
M3ZEMY	571-645-9269
M9L8YY	(571)645-9269
MDGY8V	(571) 645-9269
MHCT6X	(571) 645-9269
NDV89V	571-645-9269
NGBFWV	5716459269
NUDXH3	LazyStranger63 - In the image, lazystranger63 is tied to blackserpent34@gmail.com in tumblr, blackserpent34 is tied to Mr. Black in contacts (instagram) and Mr. Blacks number is 571-645-9269 Blackserpent34-571-645-9269 (messages has mr. black asking her to add him under blackserpent34 in hangouts) Lazystranger45- 571-645-9269 (mr. black is in contacts and has this number associated to him and this user name)
PK8DUZ	571-645-9269
QCCWH2	571-645-9269
QQ8CHV	(571)6459269
QVK6NT	5716459269
RGCV7W	571-645-9269

TABLE 1

Question 26 - Communications

WebCode	Response
RR6VHG	5716459269
T8QRYW	(571) 645-9269
TT8FBU	blackserpent34: (571) 645-9269 LazyStranger63: none recovered LazyStranger45: none recovered
UFLZ8U	571-645-9269
UQC6QQ	(571) 645-9269
URBWAT	571-645-9269
V2AL8P	(571) 645-9269
VHGMPN	(571) 645-9269
VJC6QP	(571)645-9269
VN3F2M	(571)645-9269
WWD2MW	571-645-9269
XN3Y2V	(571)645-9269
YHLTAN	LazyStranger63/blackserpent34 LazyStranger45 : (571) 645-9269
ZKATLG	LazyStranger63= not found Blackserpent34 = (Lex Luther) 571 645-9269 Lazystranger45 = 571 645-9269
ZVTJVL	blackserpent34 : 5716459269 LazyStranger45 :5716459269 LazyStranger63: 5716459269
ZWTAEN	571-645-9269

TABLE 1

Question 26 - Communications

Consensus Result: 571-645-9269

Expected Response Explanation:

In order to make this connection, messages exchanged over several messaging applications must be tracked. Messages were exchanged via Tumblr, Google Hangouts, and Skype. The messages table within these databases shows messages with respect to the application. These messages can be located at:

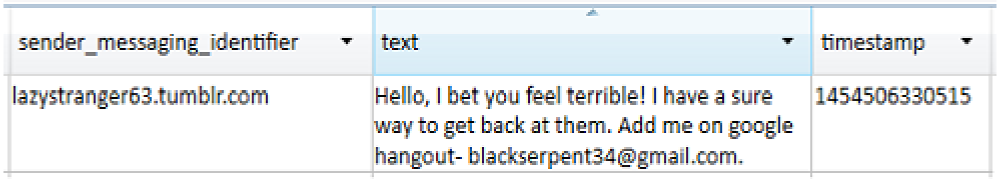
Tumblr messages:
\data\com.tumblr\databases\tumblr.sqlite

Google Hangout messages:
\data\com.google.android.talk\data\babel1.db

Skype messages:
\data\com.skype.raider\files\frosty.queen12\main.db

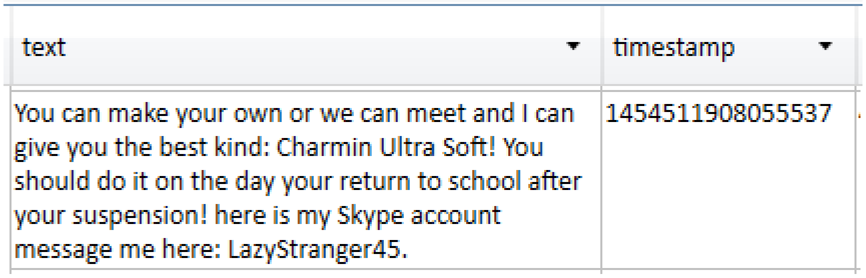
Expected Response Illustration:

Database: tumblr.sqlite >>> Table: messaging_message



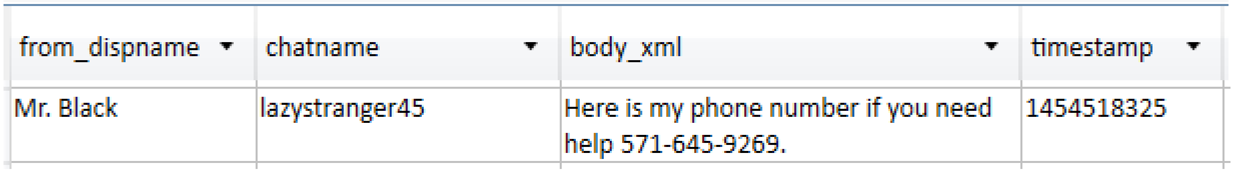
sender_messaging_identifier	text	timestamp
lazystranger63.tumblr.com	Hello, I bet you feel terrible! I have a sure way to get back at them. Add me on google hangout- blackserpent34@gmail.com.	1454506330515

Database: babel1 >>> Table: messages



text	timestamp
You can make your own or we can meet and I can give you the best kind: Charmin Ultra Soft! You should do it on the day your return to school after your suspension! here is my Skype account message me here: LazyStranger45.	1454511908055537

Database: main >>> Table: messages



from_dispname	chatname	body_xml	timestamp
Mr. Black	lazystranger45	Here is my phone number if you need help 571-645-9269.	1454518325

TABLE 1

Question 27 - Communications

Question 27: When does the first call with Lisa Frank start via Skype? (ANSWER MUST BE PRESENTED AS: DD-Month-YYYY; HH:MM:SS- UTC)

Manufacturer's Expected Response: 01 February 2016 13:49:15 UTC

WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
2EKP2R	01/02/2016 01:49:11 PM UTC	
2L4XFF	01-02-2016; 13:49:11 - UTC	
2T3MWK	01-Feb-2016;13:49:11 (-05:00 UTC)	
2ZYCPH	01-02-2016; 08:49:11 UTC-5	
3XNA9L	01/02/2016 13:49:11	
4EAWZL	01-Februari-2016; 13:49:11 UTC	
67DGNM	01-February-2016; 08:49:11 (UTC -5:00)	
6B4QXK	01-Feb-2016; 13:49:11 UTC	
6FZH7G	01-February-2016 01:49:11 PM -0 UTC	
6JJAHK	01-02-2016; 13:49:11-UTC	
6KETJL	01-February-2016; 13:49:11 UTC	
76HXLK	01- Feburary-2016 13:49:11 -0	
77PFKG	01-February-2016; 01:49:11PM	
7BNU7K	01-02-2016; 13:49:11 UTC	
7K8NDH	01-February-2016; 13:49:15- UTC	
8BHWAF	01-02-2016; 13:49:11- UTC	
8DP7RD	(01-February-2016;13:49:11 UTC)	
9AEBRE	1.02.2016 8:49:11(UTC-5)	
9CPE9B	01-February-2016; 08:49:11 (UTC-5)	
A2MFXG	01-01-2016; 13:49:11 - UTC	
AWRL2F	2/1/2016; 8:49:11 (UTC -5)	
AZRXWF	01-February-2016; 13:49:11- UTC	
B4BFFC	01-February-2016; 13:49:11 - UTC+0. (Cellebrite Extraction Report - Call Log)	
BX4PD7	01/02/2016 8:49:11 AM(UTC-5) February 1st	
C3CNWB	01-feb-2016; 13:49:11 -UTC	
C9GBYC	01-February-2016; 08:49:11 UTC-5	
D37Q26	01-Janurary-2016 13:49:11-UTC	
D8L2EA	01-February-2016; 13:49:11 UTC	
DHJ3QD	01-February-2016; 13:49:11 - UTC	
DJFH4A	01-02-2016 13:54:35 UTC+0	
DRKPJA	01-02-2016 13:49:11 UTC	
E3HPVE	01:02:2016;08:49:11	
EG36YD	01-February-2016 08:49:11 AM UTC-5	
EMVHN9	01-February-2016; 08:49:11-(UTC-5)	

TABLE 1

Question 27 - Communications

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
FWP664	01-02-2016; 13:49:11 UTC
FXKN86	1/2/2016 13:49
G63GVA	02/01/2016;01:49:11:pm(UTC+0)
GKUDX6	01/02/2016 08:49:11 UTC-5 userdata (ExtX)/Root/data/com.skype.raider/files/frosty.queen12/main.db
GNTPT6	01-February-2016; 13:49:11
GQNYD8	01-February-2016; 08:49:11 UTC-5
GRQTE7	01-Feb-16 1:49:11 PM
JZ4RHZ	01-February-2016 8:49:11 -0500 UTC
K7GAZZ	01-Feb-2016; 13:49:11
KGL8Y2	01-February-2016 13:49:11-(UTC+0)
KJ6YQY	01.02.2016 13:49:11
KJNZ38	01-February-2016 09:04:09 UTC-5
KNHWRY	01-February-2016; 13:49:11 PM-UTC+0
KUA4A8	I navigated to the Skype directory (com.skype.raider) and exported the profile folder (frosty.queen12). The profile folder was opened with the SkypeLogView application, which generated a report of the skype calls and conversations. The first call with Lisa Franks via Skype started on February 1, 2016 at 8:49:11AM. The following is the answer in the required format: - 01-February-2016; 12:49:11-UTC
KZFX43	01-february-2016; 1:49:11 AM -UTC
L66WV3	1/2/2016 DD-Month-YYYY 6:49:11 PM UTC
L6LTN3	01-February-2016 13:49:15 UTC
LYLK83	01/02/2016; 01:49:11 PM UTC
M3ZEMY	01-Feburary-2016; 08:49:11 AM -5UTC
M9L8YY	01-February-2016; 13:49:11 -UTC
MDGY8V	The first call was 01 February 2016 01:49:11 PM (UTC+0)
MHCT6X	2/1/2016 1:49:11 PM(UTC+0)
NDV89V	01-February-2016; 13:49:11- UTC
NGBFWV	01-February-2016; 01:49:11-UTC
NUDXH3	Incoming call 01-02-2016 (Feb 1, 2016) at 08:49:11 (UTC-5)
PK8DUZ	02-01-2016; 06:49:11 -0700
QCCWH2	01-FEB-2016 01:49:11 PM -UTC
QQ8CHV	01-02-2016; 13:49:11-UTC
QVK6NT	01-February-2016;13:49:11-UTC
RGCV7W	01-0202016; 13:49:11 -UTC
RR6VHG	01.02.2016 08:49:11 UTC-5
T8QRYW	01-February-2016; 13:49:11 UTC-5:00
TT8FBU	01-February-2016; 01:49:11- UTC
UFLZ8U	01-February-2016; 05:49:11 AM (UTC -8)
UQC6QQ	01-02-2016 13:54:35 UTC+0

TABLE 1

Question 27 - Communications

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
URBWAT	01-February-2016; 08:49:11 AM (-5 UTC)
V2AL8P	01-02-2016; 01:49:11 PM -UTC
VHGMPN	01-Feb-2016:08:49:11-UTC-5
VJC6QP	01-Feburary-2016 13:49:11 -UTC
VN3F2M	01-Febuary-2016; 13:49:11- UTC+0
WWD2MW	01-February-2016 13:49:11-UTC
XN3Y2V	01-02-2016 08:49:11 UTC-5
YHLTAN	Monday, 01-Feb-2016 13:49:11 UTC
ZKATLG	02-01-2016; 1:49:11 PM UTC+0
ZVTJVL	01-02-2016 13:49:11 -UTC
ZWTAEN	01-February-2016 13:49:11 UTC

TABLE 1

Question 27 - Communications

Consensus Result: ** No consensus achieved; Inconsistencies not highlighted **

Expected Response Explanation:

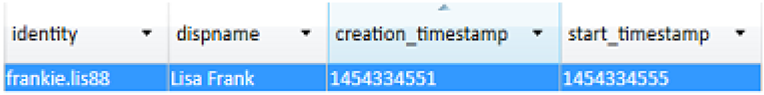
Consensus was not achieved for question 27. Majority of the responses can be placed into one group with varying conversion differences. Variations seen for this question is due to date and time conversions and response format. Below is a breakdown of the patterns seen in the responses given:

Uncoverted response for this group can be found at:
\data\com.skype.raider\files\frosty.queen12\main.db
01-February-2016; 13:49:11 UTC - 35 participants
01-Feburary-2016; 08:49:11 (UTC -5) - 18 participants
01-February-2016; 01:49:11 PM UTC - 11 participants

The question asked for the "start" time of the first call made by Lisa Frank via Skype which occurred on 01 February 2016 13:49:15 UTC. The majority of participants reported the "creation" time of the call which was 01-February-2016; 13:49:11 UTC. These participants converted the value found in the creation_timestamp field (1454334551) of the callmembers table within the main database. This field contains a timestamp stored in a Unix Epoch time format which must be converted into the requested time and date format.

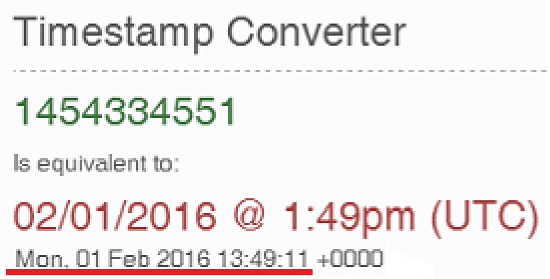
Expected Response Illustration:

Database: main >>> Table: callmembers



identity	dispname	creation_timestamp	start_timestamp
frankie.lis88	Lisa Frank	1454334551	1454334555

UTC Creation Conversion:



Timestamp Converter

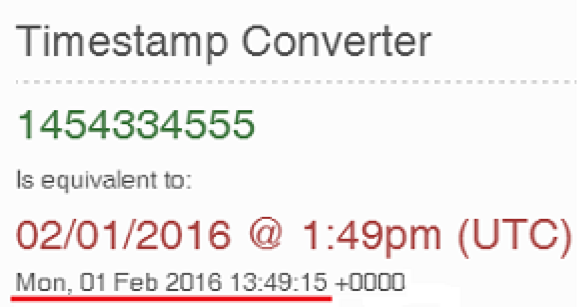
1454334551

Is equivalent to:

02/01/2016 @ 1:49pm (UTC)

Mon, 01 Feb 2016 13:49:11 +0000

UTC Start Conversion:



Timestamp Converter

1454334555

Is equivalent to:

02/01/2016 @ 1:49pm (UTC)

Mon, 01 Feb 2016 13:49:15 +0000

TABLE 1

Question 28 - Communications

Question 28: What is the phone number for Keys High School?

Manufacturer's Expected Response: 571-434-1925

WebCode	Response
2EKP2R	571-434-1925
2L4XFF	571-434-1925
2T3MWK	(571) 434-1925
2ZYCPH	571-434-1925
3XNA9L	(571) 434-1925
4EAWZL	(571) 434-1925
67DGNM	(571)434-1925
6B4QXK	+15714341925
6FZH7G	571-434-1925
6JJAHK	(571) 434-1925
6KETJL	(571) 434-1925
76HXLK	571-434-1925
77PFKG	571-434-1925
7BNU7K	(571) 434-1925
7K8NDH	(571) 434-1925
8BHWAF	571-434-1925
8DP7RD	5714341925
9AEBRE	(571) 434-1925
9CPE9B	(571)4341925
A2MFXG	(571) 434-1925
AWRL2F	(571) 434-1925
AZRXWF	571-434-1925
B4BFFC	(571) 434-1925. (Cellebrite Extraction Report - Contacts)
BX4PD7	571-434-1925
C3CNWB	(571) 434-1925
C9GBYC	(571) 434-1925
D37Q26	5714341925
D8L2EA	The phone number for the contact listed as Keys High School is (571) 434-1925
DHJ3QD	571-434-1925
DJFH4A	(571) 434-1925
DRKPJA	571-434-1925
E3HPVE	(571)-434-1925
EG36YD	(571) 434-1925
EMVHN9	(571) 434-1925
FWP664	(571)434-1925

TABLE 1

Question 28 - Communications

WebCode	Response
FXKN86	Mobile: (571) 434-1925
G63GVA	(571)434-1925
GKUDX6	5714341925 userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db
GNTPT6	(571) 434-1925
GQNYD8	(571) 434-1925
GRQTE7	5714341925
JZ4RHZ	(571) 434-1925
K7GAZZ	5714341925
KGL8Y2	5714341925
KJ6YQY	Phone number: (571) 434-1925
KJNZ38	571-4341925
KNHWRY	(571)434-1925
KUA4A8	The contacts2.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase software. Based on the analysis of this data, it is determined that the phone number associated of Keys High School is as follows: - 571-434-1925
KZFX43	(571)434-1925
L66WV3	(571) 434-1925
L6LTN3	(571)434-1925
LYLK83	(571) 434-1925
M3ZEMY	571-434-1925
M9L8YY	(571)434-1925
MDGY8V	(571) 434-1925
MHCT6X	(571) 434-1925
NDV89V	571-434-1925
NGBFWV	5714341925
NUDXH3	5714341925
PK8DUZ	571-434-1925
QCCWH2	571-434-1925
QQ8CHV	(571)4341925
QVK6NT	5714341925
RGCV7W	571-434-1925
RR6VHG	571 434 1925
T8QRYW	(571) 434-1925
TT8FBU	(571) 434-1925
UFLZ8U	571-434-1925
UQC6QQ	(571) 434-1925
URBWAT	571-434-1925
V2AL8P	(571) 434-1925

TABLE 1

Question 28 - Communications

WebCode	Response
VHGMPN	(571) 434-1925
VJC6QP	(571)434-1925
VN3F2M	(571)434-1925
WWD2MW	571-434-1925
XN3Y2V	(571)434-1925
YHLTAN	(571) 434-1925
ZKATLG	5714341925
ZVTJVL	5714341925
ZWTAEN	571-434-1925

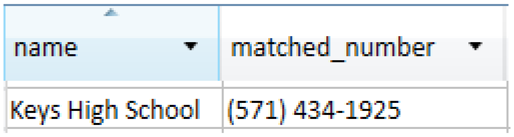
Consensus Result: 571-434-1925

Expected Response Explanation:

Information about calls made with this device can be found in the contacts2.db database. The calls table will have all of the call and contact information. The file can be found at:
\data\com.android.providers.contacts\databases\contacts2.db

Expected Response Illustration:

Database: contacts2 >>> Table: calls



name	matched_number
Keys High School	(571) 434-1925

TABLE 1

Question 29 - Communications

Question 29: How many times was Keys High School called?

Manufacturer's Expected Response: Four (4)

WebCode	Response
2EKP2R	4
2L4XFF	4
2T3MWK	4
2ZYCPH	4
3XNA9L	4
4EAWZL	4
67DGNM	4 times 2/4/2016 8:33:47 AM(UTC-5) 2/4/2016 8:27:51 AM(UTC-5) 2/3/2016 12:39:28 PM(UTC-5) 2/3/2016 12:33:27 PM(UTC-5)
6B4QXK	4
6FZH7G	4
6JJAHK	4
6KETJL	4
76HXLK	4
77PFKG	Four
7BNU7K	4
7K8NDH	4
8BHWAF	4
8DP7RD	4, but it appears that only 3 have any duration.
9AEBRE	4
9CPE9B	4
A2MFXG	4
AWRL2F	Four
AZRXWF	4
B4BFFC	Four (4). (Cellebrite Extraction Report - Contacts and Call Log)
BX4PD7	Four
C3CNWB	4
C9GBYC	Four
D37Q26	4
D8L2EA	Four (4) calls were placed to the contact listed as Keys High School
DHJ3QD	4
DJFH4A	4
DRKPJA	4
E3HPVE	4
EG36YD	4
EMVHN9	Four times

TABLE 1

Question 29 - Communications

WebCode	Response
FWP664	4
FXKN86	4 times
G63GVA	4
GKUDX6	4 userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db
GNTPT6	4
GQNYD8	4
GRQTE7	4
JZ4RHZ	4
K7GAZZ	4
KGL8Y2	4
KJ6YQY	Keys High School was called 4 times.
KJNZ38	4
KNHWRY	4
KUA4A8	The contacts2.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase software. Based on the analysis of this data, it is determined that Keys High School was called FOUR (4) times.
KZFX43	Four (4)
L66WV3	4
L6LTN3	4
LYLK83	4
M3ZEMY	4
M9L8YY	4
MDGY8V	4
MHCT6X	4
NDV89V	4
NGBFWV	4
NUDXH3	4
PK8DUZ	4
QCCWH2	4
QQ8CHV	4
QVK6NT	4
RGCV7W	4
RR6VHG	4
T8QRYW	4 (Four)
TT8FBU	4
UFLZ8U	4
UQC6QQ	4
URBWAT	4

TABLE 1

Question 29 - Communications

WebCode	Response
V2AL8P	4
VHGMPN	8
VJC6QP	4
VN3F2M	4
WWD2MW	4
XN3Y2V	4 times
YHLTAN	4
ZKATLG	8
ZVTJVL	4 times
ZWTAEN	four, however only three have an actual duration time.

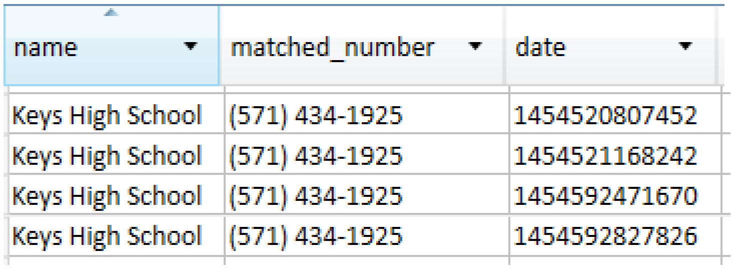
Consensus Result: Four (4)

Expected Response Explanation:

Information about calls made with this device can be found in the contacts2.db database. The calls table will have all of the call information. The file can be found at:
\data\com.android.providers.contacts\databases\contacts2.db

Expected Response Illustration:

Database: contacts2 >>> Table: calls



name	matched_number	date
Keys High School	(571) 434-1925	1454520807452
Keys High School	(571) 434-1925	1454521168242
Keys High School	(571) 434-1925	1454592471670
Keys High School	(571) 434-1925	1454592827826

TABLE 1

Question 30 - Communications

Question 30: Did Mr. Black call this device on the day it was found by police, February 4, 2016?

Manufacturer's Expected Response: Yes

WebCode	Response
2EKP2R	yes
2L4XFF	Yes
2T3MWK	Yes
2ZYCPH	Yes
3XNA9L	Yes
4EAWZL	Yes
67DGNM	Yes. 02/04/2016 8:40:15 AM
6B4QXK	Yes
6FZH7G	Yes.
6JJAHK	Yes
6KETJL	Yes
76HXLK	Yes
77PFKG	Yes
7BNU7K	Yes
7K8NDH	Yes
8BHWAF	Yes
8DP7RD	yes
9AEBRE	yes
9CPE9B	Yes
A2MFXG	Yes
AWRL2F	Yes
AZRXWF	Yes
B4BFFC	Yes, it was a "Missed Call" at 13:40:15 - UTC+0. (Cellebrite Extraction Report - Call Log)
BX4PD7	Yes
C3CNWB	Yes
C9GBYC	Yes
D37Q26	Yes
D8L2EA	Yes
DHJ3QD	yes
DJFH4A	Yes
DRKPJA	Yes
E3HPVE	Yes
EG36YD	Yes
EMVHN9	Yes
FWP664	Yes

TABLE 1

Question 30 - Communications

WebCode	Response
FXKN86	Yes, There is one missed calls from Mr. Black on 4/2/2016.
G63GVA	yes at 1:40:15PM (UTC+0)
GKUDX6	Yes he call 04/02/2016 08:40:15(UTC-5)
GNTPT6	Yes
GQNYD8	Yes
GRQTE7	yes
JZ4RHZ	Yes
K7GAZZ	Yes
KGL8Y2	Yes
KJ6YQY	Yes, Mr. Black call on „04.02.2016 13:40:15"
KJNZ38	Yes
KNHWRY	Yes
KUA4A8	The contacts2.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase software. The date and time value from the contacts2.db file were displayed in unix, therefore a unix time stamp converter was utilized to determine that Mr. Black called the device on February 4, 2016 at 8:40AM, which is the day the device was found by police. - YES - 02/04/2016 @ 1:40pm (UTC)
KZFX43	Yes
L66WV3	Yes - Missed
L6LTN3	Yes
LYLK83	Yes
M3ZEMY	Yes
M9L8YY	Yes
MDGY8V	Yes
MHCT6X	Yes
NDV89V	Yes
NGBFWV	Yes
NUDXH3	Yes, Missed call 2/4/2016 at 8:40:15 am (UTC-5)
PK8DUZ	Yes.
QCCWH2	Yes
QQ8CHV	Yes(Missed)
QVK6NT	Yes, missed call
RGCV7W	Yes
RR6VHG	Yes
T8QRYW	Yes (called but it was a missed call).
TT8FBU	yes
UFLZ8U	Yes
UQC6QQ	Yes
URBWAT	Yes

TABLE 1

Question 30 - Communications

WebCode	Response
V2AL8P	Yes
VHGMPN	Yes
VJC6QP	Yes
VN3F2M	Yes
WWD2MW	Yes
XN3Y2V	Yes
YHLTAN	yes a Missed Call at 13:40:15
ZKATLG	Yes
ZVTJVL	yes
ZWTAEN	yes

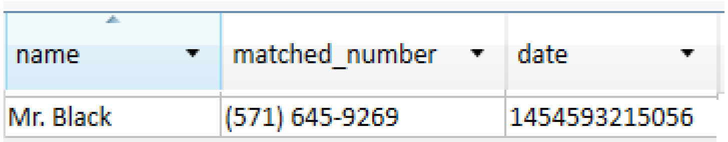
Consensus Result: Yes

Expected Response Explanation:

Information about calls can be found in the contacts2.db database or the Call Log table depending on which tool was utilized. The calls table shows information about calls related to this device. The file can be found at: \data\com.android.providers.contacts\databases\contacts2.db

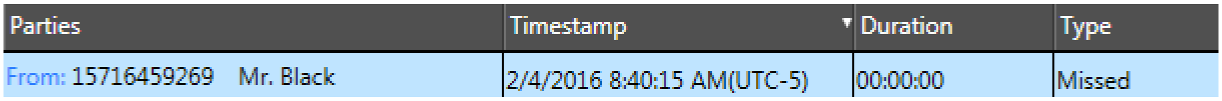
Expected Response Illustration:

Database: contacts2 >>> Table: calls



name	matched_number	date
Mr. Black	(571) 645-9269	1454593215056

Missed Call From Mr. Black Found in Call Log:



Parties	Timestamp	Duration	Type
From: 15716459269 Mr. Black	2/4/2016 8:40:15 AM(UTC-5)	00:00:00	Missed

TABLE 1

Question 31 - Communications

Question 31: How many voicemails were left on this device by contact Lisa Frank?

Manufacturer's Expected Response: Two (2)

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
2EKP2R	2
2L4XFF	0
2T3MWK	2
2ZYCPH	2
3XNA9L	None, although 2 missed calls
4EAWZL	2
67DGNM	Two voicemails
6B4QXK	2
6FZH7G	2
6JJAHK	2
6KETJL	2
76HXLK	2
77PFKG	Two
7BNU7K	2
7K8NDH	2
8BHWAF	2
8DP7RD	2
9AEBRE	zero
9CPE9B	0
A2MFXG	1
AWRL2F	None
AZRXWF	2
B4BFFC	Two (2). (data/com.metropcs.service.vvm/databases/5714658141@vms.eng.t-mobile.com.db; Messages Table)
BX4PD7	None
C3CNWB	2
C9GBYC	Two
D37Q26	2
D8L2EA	Two (2)
DHJ3QD	0
DJFH4A	0
DRKPJA	2
E3HPVE	1
EG36YD	2
EMVHN9	Two

TABLE 1

Question 31 - Communications

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
FWP664	2
FXKN86	Not found any voicemails in "main.db" file.
G63GVA	1
GKUDX6	0 userdata (ExtX)/Root/data/com.skype.raider/files/frosty.queen12/main.db
GNTPT6	2
GQNYD8	2
GRQTE7	2
JZ4RHZ	2
K7GAZZ	2
KGL8Y2	2
KJ6YQY	Two voicemails
KJNZ38	2
KNHWRY	2
KUA4A8	The 5714658141@vms.eng.t-mobile.com.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase software. The date and time value from the 5714658141@vms.eng.t-mobile.com.db file were displayed in unix, therefore a unix time stamp converter was utilized to determine that Lisa Frank left TWO (2) voicemails on this device. - Two (2) - 02/01/2016 @ 4:22pm (UTC) - 02/01/2016 @ 4:46pm (UTC)
KZFX43	Two
L66WV3	1
L6LTN3	2
LYLK83	0
M3ZEMY	2
M9L8YY	2
MDGY8V	Two
MHCT6X	2
NDV89V	2
NGBFWV	2
NUDXH3	2 voicemails Found under com.metropcs.service.vvm Data Base 5714658141@
PK8DUZ	4
QCCWH2	2
QQ8CHV	2
QVK6NT	2
RGCV7W	2
RR6VHG	2
T8QRYW	2 (Two)
TT8FBU	2
UFLZ8U	2
UQC6QQ	0

TABLE 1

Question 31 - Communications

WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
URBWAT	2	
V2AL8P	2	
VHGMPN	2	
VJC6QP	2	
VN3F2M	2	
WWD2MW	0	
XN3Y2V	None found	
YHLTAN	3	
ZKATLG	None found	
ZVTJVL	none	
ZWTAEN	two	

Consensus Result: ** No consensus achieved; Inconsistencies not highlighted **

Expected Response Explanation:

Consensus was not achieved for question 31. Majority of the responses can be placed in two response groups:

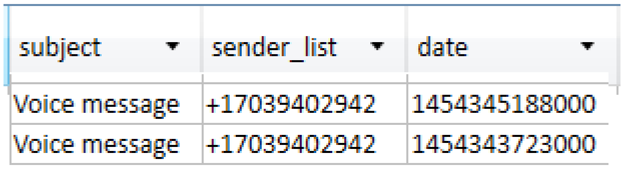
Voicemails found within the 5714658141@vms.eng.t-mobile.com.db database can be found at:
\data\com.metropcs.service.vvm\databases\5714658141@vms.eng.t-mobile.com.db
2 voicemails - 58 participants

Participants who were unable to find voicemails which could be as a result of tool dependency:
0 voicemails - 16 participants

Information about the number of voicemails can be found in the 5714658141@vms.eng.t-mobile.com.db database. The messages table will show the number of voicemails on the device. The file can be found at:
\data\com.metropcs.service.vvm\databases\5714658141@vms.eng.t-mobile.com.db

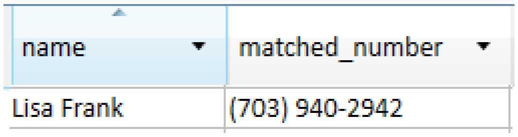
Expected Response Illustration:

Database: 5714658141@vms.eng.t-mobile.com.db Table: messages



subject	sender_list	date
Voice message	+17039402942	1454345188000
Voice message	+17039402942	1454343723000

Lisa Frank's Contact Information:



name	matched_number
Lisa Frank	(703) 940-2942

TABLE 1

Question 32 - Communications

Question 32: What does Blackserpent34 suggest that TourturedTeenageSoul88 do to their school?

Manufacturer's Expected Response: T-P the school

WebCode	Response
2EKP2R	TP the school
2L4XFF	T-P the school
2T3MWK	Blackserpent34 suggests that TourturedTeenageSoul88 should T-P the school.
2ZYCPH	T-P the school!!!
3XNA9L	Toilet Paper the school
4EAWZL	T-P the school
67DGNM	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
6B4QXK	"T-P the school"
6FZH7G	T-P the school.
6JJAHK	T-P the school!!!
6KETJL	T-P the school
76HXLK	Blackserpent34 suggest that they "T-P the school".
77PFKG	T-P the school
7BNU7K	"T-P the school" with "Charmin Ultra Soft" on the day the student returns to school after their suspension.
7K8NDH	Blackserpent34 suggests that TourturedTeenageSoul88 T-P the school.
8BHWAF	T-P the school
8DP7RD	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
9AEBRE	TP-ing
9CPE9B	He suggests to T-P the school. That's to do an act of bombing threat against the school.
A2MFXG	I suggest you T-P the school!!!
AWRL2F	"I suggest you T-P the school!!!"
AZRXWF	T-P the School.
B4BFFC	To T-P the school. (Keys High School). (Cellebrite Extraction Report - Chats)
BX4PD7	He suggests she T-P the school
C3CNWB	T-P the school
C9GBYC	T-P the school
D37Q26	T-P the school
D8L2EA	The username "TourturedTeenageSoul88" does not exist on the source media A conversation was located between "Blackserpent34" and "TorturedTeenageSoul88" In the conversation the suggestion made is to "T-P the school"
DHJ3QD	T-P the school

TABLE 1

Question 32 - Communications

WebCode	Response
DJFH4A	T-P the school
DRKPJA	T-P the school
E3HPVE	Blackserpent34 suggest that TourturedTeenageSoul88 to T-P (Toilet Paper) the school.
EG36YD	T-P the school!!
EMVHN9	Blackserpent34 suggested the following: “Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!”
FWP664	T-P the school
FXKN86	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
G63GVA	"I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!"
GKUDX6	I suggest you T-P the school!!! userdata (ExtX)/Root/data/com.google.android.talk/databases/babel1.db
GNTPT6	To T-P the school.
GQNYD8	TP school
GRQTE7	suggest T-P the school
JZ4RHZ	T-P the school
K7GAZZ	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
KGL8Y2	T-P the school!!!
KJ6YQY	”T-P the school”
KJNZ38	T-P the school
KNHWRY	He suggests that she should T-P the school.
KUA4A8	The babel1.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser. Based on the analysis of this data, it is determined that Blackserpent34 suggested the following to TorturedTeenageSoul88: - "Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way!! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!"
KZFX43	Blackserpent34 suggests to T-P the school
L66WV3	suggest T-P the school
L6LTN3	T-P the school on the day she returns to school after suspension
LYLK83	T-P
M3ZEMY	T-P the school
M9L8YY	T-P the school

TABLE 1

Question 32 - Communications

WebCode	Response
MDGY8V	“Yes I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
MHCT6X	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
NDV89V	T-P the school
NGBFWV	T-P the school
NUDXH3	T-Ping the school
PK8DUZ	T-P the school.
QCCWH2	T-P the school!!!
QQ8CHV	Toliet-Papering the school
QVK6NT	T-P the school
RGCV7W	T-P the school
RR6VHG	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
T8QRYW	“I suggest you T-P the school!!!”
TT8FBU	"I suggest you T-P the school"
UFLZ8U	T-P the school.
UQC6QQ	T-P the school
URBWAT	Blackserpent34 suggests that TorturedTeenageSoul88 T-P's the school.
V2AL8P	Bombing the school
VHGMPN	T-P the school
VJC6QP	T-P the school
VN3F2M	T-P the school
WWD2MW	"I suggest you T-P the school!!!"
XN3Y2V	T-P the school
YHLTAN	Blackserpent34 suggest that TourturedTeenageSoul88 "toilet-papering the school".
ZKATLG	I suggest you T-P the school. (or bomb the school with the case scenario)
ZVTJVL	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
ZWTAEN	TP it

TABLE 1

Question 32 - Communications

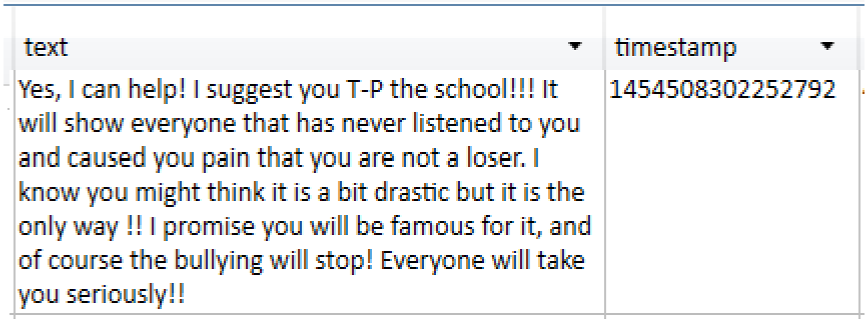
Consensus Result: T-P the school

Expected Response Explanation:

Information about messages sent via google hangouts can be seen in the babel1.db database. The messages table will show message content. This information can be found at:
\data\com.google.android.talk\data\babel1.db

Expected Response Illustration:

Database: babel1 >>> Table: messages



text	timestamp
Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!	1454508302252792

TABLE 1

Question 33 - Communications

Question 33: What is the name of the attachment Diane Chambers sends in a group e-mail?

Manufacturer's Expected Response: Falling_Stella.jpg

WebCode	Response
2EKP2R	Falling_Stella.jpg
2L4XFF	Falling_Stella.jpg
2T3MWK	Falling_Stella.jpg
2ZYCPH	Falling_Stella.jpg
3XNA9L	Falling_Stella.jpg
4EAWZL	Falling_Stella.jpg
67DGNM	Falling_Stella.jpg
6B4QXK	Falling_Stella.jpg
6FZH7G	Falling_Stella.jpg
6JJAHK	Falling_Stella.jpg
6KETJL	Falling_Stella.jpg
76HXLK	Falling_Stella.jpg
77PFKG	Falling_Stella.jpg
7BNU7K	Falling_Stella.jpg
7K8NDH	Falling_Stella.jpg
8BHWAF	Falling_Stella.jpg
8DP7RD	Falling_Stella.jpg
9AEBRE	Falling_Stella.jpg
9CPE9B	Falling_Stella-jpg
A2MFXG	Falling_Stella.jpg
AWRL2F	Falling_Stella.jpg
AZRXWF	Falling_Stella.jpg
B4BFFC	Falling_Stella.jpg. (Cellebrite Extraction Report - Emails)
BX4PD7	Falling_Stella.jpg
C3CNWB	Falling_Stella.jpg
C9GBYC	Falling_Stella.jpg
D37Q26	Falling_Stella.jpg
D8L2EA	Falling_Stella.jpg
DHJ3QD	Falling_Stella.jpg
DJFH4A	Falling_Stella.jpg
DRKPJA	Falling_Stella
E3HPVE	Falling_Stella.jpg
EG36YD	Falling_Stella.jpg
EMVHN9	Falling_Stella.jpg
FWP664	falling_stella.jpg

TABLE 1

Question 33 - Communications

WebCode	Response
FXKN86	Falling_Stella.jpg
G63GVA	Falling_Stella.jpg
GKUDX6	Falling_stella.jpg
GNTPT6	Falling_Stella.jpg
GQNYD8	Falling_Stella.jpg
GRQTE7	Falling_Stella.jpg
JZ4RHZ	Falling_Stella.jpg
K7GAZZ	Falling_Stella.jpg
KGL8Y2	Falling_Stella.jpg
KJ6YQY	Falling_Stella.jpg, Falling_Stella-1.jpg
KJNZ38	Falling_Stella.jpg
KNHWRY	Falling_Stella.jpg
KUA4A8	The mailstore.st3llar8@gmail.com.db file was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase 7. Based on the analysis of this data, it is determined that the following attachment was sent from Diane Chambers in a group email: - Falling_Stella.jpg
KZFX43	Falling_Stella.jpg
L66WV3	falling_stella.jpg
L6LTN3	Falling_Stella.jpg
LYLK83	Falling_Stella.jpg
M3ZEMY	Falling_Stella.jpg
M9L8YY	Falling_Stella.jpg
MDGY8V	Falling_Stella.jpg
MHCT6X	Falling_Stella.jpg
NDV89V	Falling_Stella.jpg
NGBFWV	Falling_Stella.jpg
NUDXH3	Falling_Stell.jpg
PK8DUZ	Falling_Stella.jpg
QCCWH2	Falling_Stella.jpg
QQ8CHV	Falling_Stella.jpg
QVK6NT	Falling_Stella.jpg
RGCV7W	Falling_Stella.jpg
RR6VHG	Falling_Stella.jpg
T8QRYW	Falling_Stella.jpg
TT8FBU	Falling_Stella.jpg
UFLZ8U	Falling_Stella.jpg
UQC6QQ	Falling_Stella.jpg
URBWAT	Falling_Stella.jpg
V2AL8P	Falling_Stella.jpg

TABLE 1

Question 33 - Communications

WebCode	Response
VHGMPN	Falling_Stella.jpg
VJC6QP	Falling_Stella.jpg
VN3F2M	Falling_Stella.jpg
WWD2MW	Falling_Stella.jpg
XN3Y2V	Falling_Stella.jpg
YHLTAN	Falling_Stella.jpg
ZKATLG	Falling_Stella.jpg
ZVTJVL	/data/data/com.google.android.gm/cache/st3llar8@gmail.com/falling_stella.jpg
ZWTAEN	Falling-Stella.jpg

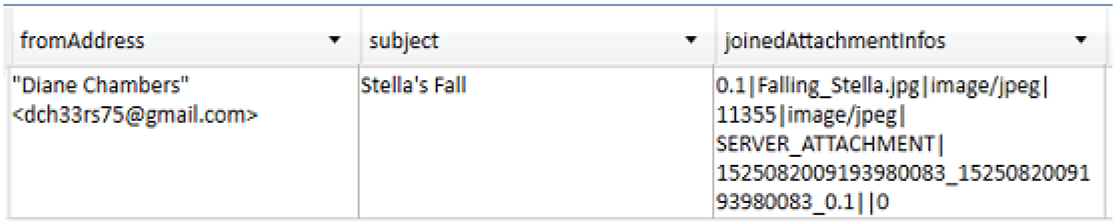
Consensus Result: Falling_Stella.jpg

Expected Response Explanation:

Information about e-mail attachments for g-mail can be found in the mailstore.st3llar8@gmail.com.db database. The messages table will show file attachment data. The file can be found at:
\data\com.google.android.gm\databases\mailstore.st3llar8@gmail.com

Expected Response Illustration:

Database: mailstore.st3llar8@gmail.com >>> Table: messages



<table>
<tr><th>fromAddress</th><th>subject</th><th>joinedAttachmentInfos</th></tr>
<tr><td>"Diane Chambers" <dch33rs75@gmail.com></td><td>Stella's Fall</td><td>0.1|Falling_Stella.jpg|image/jpeg|11355|image/jpeg|SERVER_ATTACHMENT|1525082009193980083_1525082009193980083_0.1||0</td></tr>
</table>

TABLE 1

Question 34 - Communications

Question 34: What is the google e-mail address associated with this device? (ANSWER MUST BE PROVIDED AS FULL ADDRESS)

Manufacturer's Expected Response: st3llar8@gmail.com

WebCode	Response
2EKP2R	st3llar8@gmail.com
2L4XFF	st3llar8@gmail.com
2T3MWK	st3llar8@gmail.com
2ZYCPH	st3llar8@gmail.com
3XNA9L	st3llar8@gmail.com
4EAWZL	st3llar8@gmail.com
67DGNM	st3lar8@gmail.com
6B4QXK	st3llar8@gmail.com
6FZH7G	st3llar8@gmail.com
6JJAHK	st3llar8@gmail.com
6KETJL	st3llar8@gmail.com
76HXLK	st3llar8@gmail.com
77PFKG	st3llar8@gmail.com
7BNU7K	st3llar8@gmail.com
7K8NDH	st3llar8@gmail.com
8BHWAF	st3llar8@gmail.com
8DP7RD	st3llar8@gmail.com
9AEBRE	st3llar8@gmail.com
9CPE9B	st3llar8@gmail.com
A2MFXG	st3llar8@gmail.com
AWRL2F	st3llar8@gmail.com
AZRXWF	st3llar8@gmail.com
B4BFFC	st3llar8@gmail.com. (Cellebrite Extraction Report - User Accounts)
BX4PD7	St3llar8@gmail.com
C3CNWB	st3llar8@gmail.com
C9GBYC	st3llar8@gmail.com
D37Q26	st3llar8@gmail.com
D8L2EA	st3llar8@gmail.com
DHJ3QD	st3llar8@gmail.com
DJFH4A	st3llar8@gmail.com
DRKPJA	st3llar8@gmail.com
E3HPVE	st3llar8@gmail.com
EG36YD	st3llar8@gmail.com
EMVHN9	St3llar8@gmail.com

TABLE 1

Question 34 - Communications

WebCode	Response
FWP664	st3llar8@gmail.com
FXKN86	st3llar8@gmail.com
G63GVA	st3llar8@gmail.com
GKUDX6	St3llar8@gmail.com
GNTPT6	st3llar8@gmail.com
GQNYD8	st3llar8@gmail.com
GRQTE7	st3llar8@gmail.com
JZ4RHZ	st3llar8@gmail.com
K7GAZZ	st3llar8@gmail.com
KGL8Y2	st3llar8@gmail.com
KJ6YQY	Account Name: st3llar8@gmail.com
KJNZ38	st3llar8@gmail.com
KNHWRY	st3llar8@gmail.com
KUA4A8	The contacts2.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase software. Based on the analysis of this data, it is determined that the Google email address associated with this device is as follows: - st3llar8@gmail.com
KZFX43	st3llar8@gmail.com
L66WV3	st3llar8@gmail.com
L6LTN3	st3llar8@gmail.com
LYLK83	st3llar8@gmail.com
M3ZEMY	st3llar8@gmail.com
M9L8YY	st3llar8@gmail.com
MDGY8V	“Stella Frost" st3llar8@gmail.com”
MHCT6X	st3llar8@gmail.com
NDV89V	St3llar8@gmail.com
NGBFWV	st3llar8@gmail.com
NUDXH3	St3llar8@gmail.com
PK8DUZ	st3llar8@gmail.com
QCCWH2	st3llar8@gmail.com
QQ8CHV	st3llar8@gmail.com
QVK6NT	st3llar8@gmail.com
RGCV7W	st3llar8@gmail.com
RR6VHG	st3llar8@gmail.com
T8QRYW	St3llar8@gmail.com
TT8FBU	st311ar8@gmail.com
UFLZ8U	st3llar8@gmail.com
UQC6QQ	st3llar8@gmail.com
URBWAT	st3llar8@gmail.com

TABLE 1

Question 34 - Communications

WebCode	Response
V2AL8P	st3llar8@gmail.com
VHGMPN	st3llar8@gmail.com
VJC6QP	st3llar8@gmail.com
VN3F2M	St3llar8@gmail.com
WWD2MW	st3llar8@gmail.com
XN3Y2V	st3llar8@gmail.com
YHLTAN	st3llar8@gmail.com
ZKATLG	St3llar8@gmail.com
ZVTJVL	st3llar8@gmail.com
ZWTAEN	st3llar8@gmail.com

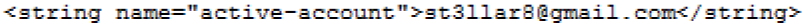
Consensus Result: st3llar8@gmail.com

Expected Response Explanation:

Information about the active G-Mail account can be found in the Gmail.xml file. In this file there is a string name "Active-account" with the value st3llar8@gmail.com. This file can be found at:
\data \com.google.android.gm\shared_prefs\Gmail.xml.

Expected Response Illustration:

Active Gmail Account:



```
<string name="active-account">st3llar8@gmail.com</string>
```

TABLE 1

Question 35 - Communications

Question 35: What is the Yahoo e-mail address associated with this device?

Manufacturer's Expected Response: notyouraveragejoe78@yahoo.com

WebCode	Response
2EKP2R	notyouraveragejoe78@yahoo.com
2L4XFF	Notyouraveragejoe78@yahoo.com
2T3MWK	notyouravaragejoe78@yahoo.com
2ZYCPH	notyouraveragejoe78@yahoo.com
3XNA9L	notyouraveragejoe78@yahoo.com
4EAWZL	notyouraveragejoe78@yahoo.com
67DGNM	notyouraveragejoe78@yahoo.com
6B4QXK	notyouraveragejoe78@yahoo.com
6FZH7G	notyouraveragejoe78@yahoo.com
6JJAHK	notyouraveragejoe78@yahoo.com
6KETJL	notyouaveragejoe78@yahoo.com
76HXLK	notyouraveragejoe78@yahoo.com
77PFKG	notyouraveragejoe78@yahoo.com
7BNU7K	notyouraveragejoe78@yahoo.com
7K8NDH	notyouraveragejoe78@yahoo.com
8BHWAF	notyouraveragejoe78@yahoo.com
8DP7RD	notyouraveragejoe78@yahoo.com
9AEBRE	notyouraveragejoe78@yahoo.com
9CPE9B	notyouraveragejoe@yahoo.com
A2MFXG	notyouraveragejoe78@yahoo.com
AWRL2F	notyouraveragejoe78@yahoo.com
AZRXWF	notyouraveragejoe78@yahoo.com
B4BFFC	The Yahoo e-mail address associated with this device is "notyouraveragejoe78@yahoo.com". (1.db, Message table)
BX4PD7	Notyouraveragejoe78@yahoo.com
C3CNWB	notyouraveragejoe78@yahoo.com
C9GBYC	notyouraveragejoe78@yahoo.com
D37Q26	notyouraveragejoe78@yahoo.com
D8L2EA	notyouraveragejoe78@yahoo.com
DHJ3QD	notyouraveragejoe78@yahoo.com
DJFH4A	MAILER-DAEMON@yahoo.com
DRKPJA	notyouraveragejoe78@yahoo.com
E3HPVE	notyouraveragejoe78@yahoo.com
EG36YD	notyouraveragejoe78@yahoo.com
EMVHN9	notyouraveragejoe78@yahoo.com

TABLE 1

Question 35 - Communications

WebCode	Response
FWP664	notyouraveragejoe78@yahoo.com
FXKN86	notyouraveragejoe78@yahoo.com
G63GVA	notyouraveragejoe78@yahoo.com This email was found to have the source account of st3llar8@gmial.com (Stella Frost)
GKUDX6	Notyouraveragejoe78@yahoo.com userdata (ExtX)/Root/data/com.android.browser/app_ace/databases/Databases.db
GNTPT6	notyouraveragejoe78@yahoo.com
GQNYD8	notyouraveragejoe78@yahoo.com
GRQTE7	notyouraveragejoe78@yahoo.com
JZ4RHZ	notyouraveragejoe78@yahoo.com
K7GAZZ	notyouraveragejoe78@yahoo.com
KGL8Y2	notyouraveragejoe78@yahoo.com
KJ6YQY	notyouraveragejoe78@yahoo.com
KJNZ38	notyouraveragejoe78@yahoo.com
KNHWRY	notyouraveragejoe78@yahoo.com
KUA4A8	The contacts2.db file and additional contact data was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase software. Based on the analysis of this data, it is determined that the Yahoo email address associated with this device is as follows: - notyouraveragejoe78@yahoo.com
KZFX43	notyouraveragejoe78@yahoo.com
L66WV3	notyouraveragejoe78@yahoo.com
L6LTN3	notyouraveragejoe78@yahoo.com
LYLK83	notyouraveragejoe78@yahoo.com
M3ZEMY	notyouraveragejoe78@yahoo.com
M9L8YY	notyouraveragejoe78@yahoo.com
MDGY8V	notyouraveragejoe78@yahoo.com
MHCT6X	notyouraveragejoe78@yahoo.com
NDV89V	Notyouraveragejoe78@yahoo.com
NGBFWV	notyouraveragejoe78@yahoo.com
NUDXH3	notyouraveragejoe78@yahoo.com
PK8DUZ	notyouraveragejoe78@yahoo.com
QCCWH2	notyouraveragejoe78@yahoo.com
QQ8CHV	
QVK6NT	Notyouraveragejoe78@yahoo.com
RGCV7W	notyouraveragejoe78@yahoo.com
RR6VHG	notyouraveragejoe78@yahoo.com MAILER-DAEMON@yahoo.com
T8QRYW	Notyouraveragejoe78@yahoo.com
TT8FBU	notyouraveragejoe78@yahoo.com
UFLZ8U	notyouraveragejoe78@yahoo.com

TABLE 1

Question 35 - Communications

WebCode	Response
UQC6QQ	MAILER-DAEMON@yahoo.com
URBWAT	notyouraveragejoe78@yahoo.com
V2AL8P	notyouraveragejoe78@yahoo.com
VHGMPN	notyouraveragejoe78@yahoo.com
VJC6QP	notyouraveragejoe78@yahoo.com
VN3F2M	notyouraveragejoe78@yahoo.com
WWD2MW	notyouraveragejoe78@yahoo.com
XN3Y2V	notyouraveragejoe78@yahoo.com
YHLTAN	none
ZKATLG	Notyouraveragejoe78@yahoo.com
ZVTJVL	E-mail: notyouraveragejoe78@yahoo.com
ZWTAEN	notyouraveragejoe78@yahoo.com

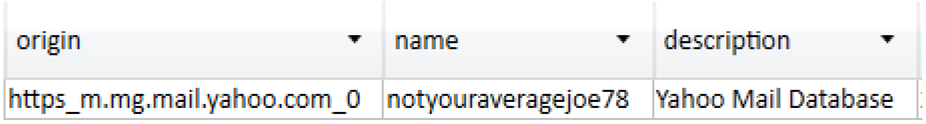
Consensus Result: notyouraveragejoe78@yahoo.com

Expected Response Explanation:

Information about the yahoo e-mail account that was accessed via the internet can be found at the databases.db database. The databases table contains a name column with the value "notyouraveragejoe78." This file can be found at:
\data\com.android.browser\app_ace\databases\databases.db

Expected Response Illustration:

Database: databases >>> Table: databases



origin	name	description
https_m.mg.mail.yahoo.com_0	notyouraveragejoe78	Yahoo Mail Database

TABLE 1

Question 36 - Communications

Question 36: How many e-mails were sent using the Yahoo account?

Manufacturer's Expected Response: Three (3)

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
2EKP2R	3 emails were sent
2L4XFF	6
2T3MWK	3
2ZYCPH	3
3XNA9L	3
4EAWZL	3
67DGNM	Three
6B4QXK	3, including 1 failed
6FZH7G	3
6JJAHK	6
6KETJL	3
76HXLK	3
77PFKG	Three
7BNU7K	6
7K8NDH	3
8BHWAF	3
8DP7RD	3
9AEBRE	3
9CPE9B	1
A2MFXG	6
AWRL2F	None
AZRXWF	1
B4BFFC	There are three (3) e-mails sent from "notyouraveragejoe78@yahoo.com" to "KeysHighSchool". However, the "Folder" database lists that six (6) e-mails were sent. It is unclear if all six (6) e-mails were sent from the Yahoo account. (1.db, Folder and Message tables)
BX4PD7	One email was sent to the yahoo address from the st3llar8@gmail.com account. However no emails sent from the yahoo account were observed.
C3CNWB	3
C9GBYC	Three
D37Q26	3
D8L2EA	Three (3)
DHJ3QD	0
DJFH4A	6
DRKPJA	6
E3HPVE	4
EG36YD	1

TABLE 1

Question 36 - Communications

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
EMVHN9	Six emails were sent from the email account, notyouraveragejoe78@yahoo.com.
FWP664	3
FXKN86	Not found. E-mail were sent using the yahoo account except two e-mails were sent from "st3llar8@gmail.com" to "notyouraveragejoe78@yahoo.com". However we found login yahoo account via Android system browser.
G63GVA	3
GKUDX6	3 userdata (ExtX)/Root/data/com.android.browser/app_ace/databases/https_m.mg.mail.yahoo.com_0/1
GNTPT6	3
GQNYD8	3
GRQTE7	0
JZ4RHZ	3 emails
K7GAZZ	3
KGL8Y2	3
KJ6YQY	Three e-mails
KJNZ38	3
KNHWRY	3
KUA4A8	The mailstore.st3llar8@gmail.com.db file was located, then exported to the target drive and viewed with SQLiteBrowser and EnCase 7. Based on the analysis of this data, it is determined that ONE (1) email was sent using the Yahoo account, which is as follows: - ONE (1) - "Subject = Keys" - "To whom it may concern, on 2/4/2016 there will be a T-Ping of the school! You have been warned!"
KZFX43	Three (3)
L66WV3	1
L6LTN3	3
LYLK83	3
M3ZEMY	3
M9L8YY	1
MDGY8V	3
MHCT6X	3
NDV89V	3
NGBFWV	3
NUDXH3	one: "on 2/4/2016 there will be a T-Ping of the school! you have been warned!"
PK8DUZ	1
QCCWH2	4
QQ8CHV	
QVK6NT	3
RGCV7W	1
RR6VHG	4 (included mailer daemon)
T8QRYW	3 (Three)
TT8FBU	3

TABLE 1

Question 36 - Communications

WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
UFLZ8U	3 emails were sent	
UQC6QQ	6	
URBWAT	3	
V2AL8P	1	
VHGMPN	6	
VJC6QP	3	
VN3F2M	3	
WWD2MW	1	
XN3Y2V	one	
YHLTAN	01	
ZKATLG	0	
ZVTJVL	1	
ZWTAEN	three	

TABLE 1

Question 36 - Communications

Consensus Result: ** No consensus achieved; Inconsistencies not highlighted **

Expected Response Explanation:

Consensus was not achieved for question 36. Majority of the responses can be placed in three response groups:

E-mails found in the messages table within the 1.db database can be found at:
\data\com.android.browser\app_ace\databases\https_m.mg.mail.yahoo.com_0\1.db
3 e-mails - 47 participants

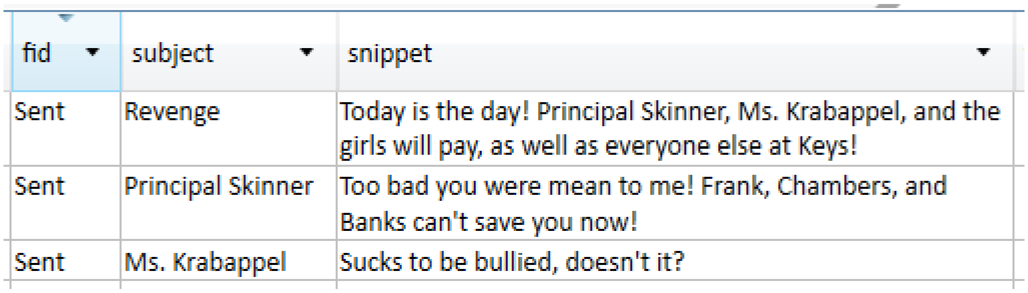
Total number of e-mails sent via folder table within the 1.db database can be found at:
\data\com.android.browser\app_ace\databases\https_m.mg.mail.yahoo.com_0\1.db
6 e-mails - 9 participants

Additional responses included:
1 e-mail - 14 participants
0 e-mails - 6 participants

Information on yahoo e-mails can be found in the 1.db database. The messages table will contain information about e-mails sent. The folder table contains information about total number of e-mails sent. This file can be found at:
\data\com.android.browser\app_ace\databases\https_m.mg.mail.yahoo.com_0\1.db

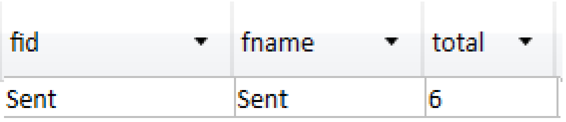
Expected Response Illustration:

Database: 1 >>> Table: messages



fid	subject	snippet
Sent	Revenge	Today is the day! Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!
Sent	Principal Skinner	Too bad you were mean to me! Frank, Chambers, and Banks can't save you now!
Sent	Ms. Krabappel	Sucks to be bullied, doesn't it?

Database: 1 >>> Table: folder



fid	fname	total
Sent	Sent	6

TABLE 1

Question 37 - Analysis

Question 37: From your analysis what is the name associated with the primary accounts on this device?

Manufacturer's Expected Response: Stella Frost

WebCode	Response
2EKP2R	Stella Frost
2L4XFF	Stella Frost
2T3MWK	Stella Frost
2ZYCPH	Stella Frost
3XNA9L	Stella Frost
4EAWZL	Stella Frost
67DGNM	Stella Frost
6B4QXK	Stella Frost
6FZH7G	Stella Frost
6JJAHK	Stella Frost
6KETJL	Stella Frost
76HXLK	Stella Frost
77PFKG	Stella Frost
7BNU7K	Stella Frost
7K8NDH	Stella Frost
8BHWAF	Stella Frost
8DP7RD	Stella Frost
9AEBRE	Stella Frost
9CPE9B	Stella Frost
A2MFXG	Stella Frost
AWRL2F	STELLA FROST
AZRXWF	Stella Frost
B4BFFC	Stella Frost; Gmail: st3llar8@gmail.com; Skype: frosty.queen12; Google Hangouts: Alpha Beta; Yahoo Account: notyouraveragejoe78@yahoo.com (Cellebrite Extraction Report)
BX4PD7	Stella Frost
C3CNWB	Stella Frost
C9GBYC	Stella Frost. This name is directly associated with social media accounts--Google+, Hangouts, Skype and Instagram--on this device and is consistent with the name on the suspension slip. This name is also indirectly associated with other accounts on this device--Tumblr, Gmail, Google Maps and Yahoo mail ("Stel Fro").
D37Q26	Stella Frost
D8L2EA	Stella Frost
DHJ3QD	Stella Frost
DJFH4A	Stella Frost
DRKPJA	Stella Frost
E3HPVE	Stella Frost

TABLE 1

Question 37 - Analysis

WebCode	Response
EG36YD	Stella Frost
EMVHN9	The name associated is Stella Frost.
FWP664	Stella Frost
FXKN86	FullName is "Stella Frost" or E-mail : "st3llar8@gmail.com"
G63GVA	Stella Frost
GKUDX6	st3llar8@gmail.com gmail frosty.queen12 skype torturedteenagesoul88 Tumblr Notyouraveragejoe78@yahoo.com yahoo
GNTPT6	Stella Frost
GQNYD8	Stella Frost
GRQTE7	Stella Frost
JZ4RHZ	Stella Frost
K7GAZZ	Stella Frost
KGL8Y2	Stella Frost
KJ6YQY	Stella Frost
KJNZ38	Stella Frost
KNHWRY	Stella Frost
KUA4A8	Based on the analysis of this data, it is determined that STELLA FROST is the name associated with the primary accounts on this device. Such accounts are as follows: 1. Tumblr - torturedteenagesoul88.tumblr.com 2. Gmail - st3llar8@gmail.com 3. Skype - frosty.queen12
KZFX43	Stella Frost
L66WV3	Stella Frost
L6LTN3	Stella Frost
LYLK83	Stella Frost
M3ZEMY	Stella Frost
M9L8YY	Stella Frost
MDGY8V	Stella Frost
MHCT6X	Stella Frost
NDV89V	Stella Frost
NGBFWV	Stella Frost
NUDXH3	Stella Frost
PK8DUZ	Stella Frost
QCCWH2	Stella Frost
QQ8CHV	Stella Frost, st3llar8@gmail.com
QVK6NT	Stella Frost
RGCV7W	Stella Frost
RR6VHG	Tumblr = Torturedteenagesoul88 Google = St3llar8@gmail.com Hangout = Alpha Beta; St3llar8@gmail.com Skype = Frosty.queen12 phone = lge
T8QRYW	Stella Frost
TT8FBU	Stella Frost

TABLE 1

Question 37 - Analysis

WebCode	Response
UFLZ8U	Stella Frost
UQC6QQ	Stella Frost
URBWAT	Stella Frost
V2AL8P	Stella Frost
VHGMPN	Stella Frost
VJC6QP	Stella Frost
VN3F2M	Stella Frost
WWD2MW	Stella Frost
XN3Y2V	Stella Frost
YHLTAN	Stella Frost
ZKATLG	Stella Frost
ZVTJVL	st3llar8@gmail.com Stella Frost
ZWTAEN	Stella Frost

TABLE 1

Question 37 - Analysis

Consensus Result: Stella Frost

Expected Response Explanation:

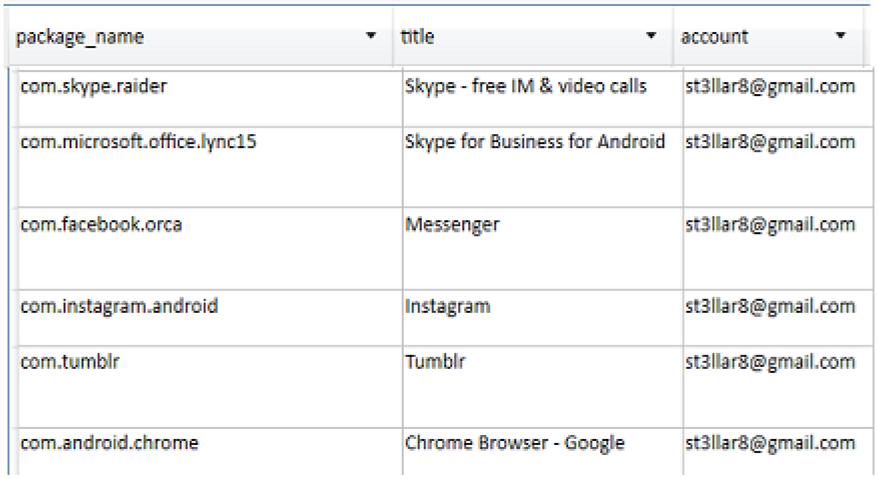
The account that downloaded the applications onto this device can be found in the localappstate.db database. The appstate table shows primary account information, st3llar8@gmail.com. This file can be found at:
data\com.android.vending\databases\localappstate.db

The name associated to that account is Stella Frost. This information can be found at:
\data\com.google.android.talk\data\babel1.db

In Tumblr, torturedteenagesoul88 gives out the google account of st3llar8@gmail.com, which is linked to the name Stella Frost. This information can be found at:
\data\com.tumblr\databases\tumblr.sqlite

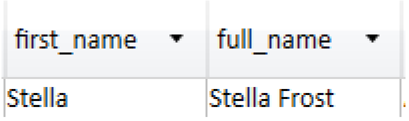
Expected Response Illustration:

Database: localappstate >>> Table: appstate



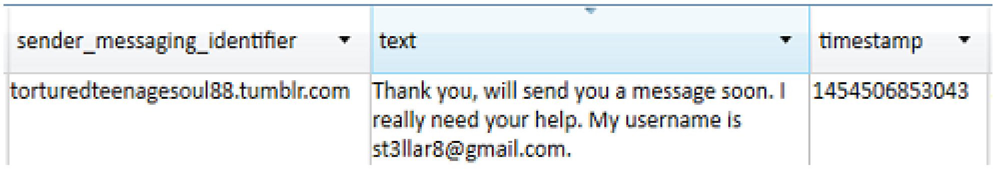
package_name	title	account
com.skype.raider	Skype - free IM & video calls	st3llar8@gmail.com
com.microsoft.office.lync15	Skype for Business for Android	st3llar8@gmail.com
com.facebook.orca	Messenger	st3llar8@gmail.com
com.instagram.android	Instagram	st3llar8@gmail.com
com.tumblr	Tumblr	st3llar8@gmail.com
com.android.chrome	Chrome Browser - Google	st3llar8@gmail.com

Database: babel1 >>> Table: participants



first_name	full_name
Stella	Stella Frost

Database: tumblr.sqlite >>> Table: messages



sender_messaging_identifier	text	timestamp
torturedteenagesoul88.tumblr.com	Thank you, will send you a message soon. I really need your help. My username is st3llar8@gmail.com.	1454506853043

TABLE 1

Question 38 - Analysis

Question 38: From your analysis was this device used to plan for the toilet papering of Keys High School?

Manufacturer's Expected Response: Yes

WebCode	Response
2EKP2R	yes
2L4XFF	Yes
2T3MWK	Yes. Several artifacts were found including searches of TP-ing, threats and conversations of TP-ing.
2ZYCPH	Yes
3XNA9L	Yes from messages on 03/02/2016 via skype also outgoing email 'To whom it may concern', sms to arrange collection of toilet paper
4EAWZL	Yes
67DGNM	Yes. The analysis revealed that not only was the device used to make the threat to Keys High School but it was used to gather information through contacts on social media, internet searches, and download of applications for use in concealing the identity of the attacker.
6B4QXK	Yes
6FZH7G	Yes
6JJAHK	Yes
6KETJL	Yes
76HXLK	Yes
77PFKG	Yes
7BNU7K	Yes
7K8NDH	Yes. There are conversations within Tumblr, Hangouts, Skype and the native Messages application which contain both incoming and outgoing messages about the device user being bullied, wanting revenge and talking about T-Ping the school with a third party. There is one image within the 'Downloads' folder which gives instructions about making your own toilet paper. Multiple images of toilet paper have been extracted from cache and carved from memory. One of these images appears to show a drawing of Keys High School with toilet paper next to it.
8BHWAF	Yes
8DP7RD	yes
9AEBRE	yes
9CPE9B	Yes
A2MFXG	Yes
AWRL2F	Yes
AZRXWF	Yes
B4BFFC	Yes, from my analysis this device was used to plan for the toilet papering of Keys High School. Data recovered from the device showed that the phone was used to research information for the toilet papering event, as well as, used to contact Keys High School to make threats and obtain information from others as to how to go about the toilet papering event.
BX4PD7	Yes
C3CNWB	Yes
C9GBYC	Yes. The data--such as calendar events, call log, alarm memos, web searches, third-party application chat threads and pictures--found on the submitted image file suggest this device may have been used to plan for the toilet papering of Keys High School.

TABLE 1

Question 38 - Analysis

WebCode	Response
D37Q26	Yes
D8L2EA	Yes
DHJ3QD	yes there is planning taking place for a TP-ing event.
DJFH4A	Yes
DRKPJA	Yes
E3HPVE	Yes
EG36YD	Yes
EMVHN9	Yes, communication and multimedia messages were exchanged with this device regarding the toilet papering of Keys High School.
FWP664	Yes
FXKN86	Yes, Because some messages, pictures and data searching concern with the word "Toilet papering" were found via AppChat and web brownser.
G63GVA	yes, There are e-mails threatening the T-Ping of the school. There are also chats with information about t-ping, and a chat that says "Yes, I am going to T-P Keys High School" Also located were web histories for T-P. There were also several browser activities for T-P related sites. Analysis also revealed several T-Ping and T-P related search terms. Also located several images related to T-P.
GKUDX6	yes
GNTPT6	Yes
GQNYD8	Yes
GRQTE7	yes
JZ4RHZ	Yes, this device contains chats, emails, and Internet history referencing Keys Highs School and targets to toilet paper the school.
K7GAZZ	Yes
KGL8Y2	Yes
KJ6YQY	Yes
KJNZ38	Yes
KNHWRY	Yes
KUA4A8	YES, based on my analysis of this evidence, I have determined that this device was used to plan for the toilet papering of Keys High School. To support my determination, I will specifically point to the following: - Skype communication between frosty.queen12 (STELLA FROST) and lazystranger45 (Mr. Black) pertaining to the toilet papering of the school. Specifically, when the individual using the profile of STELLA FROST told Mr. Black that she was going to T-P Keys High School. - A yahoo email account (notyouraveragejoe78@yahoo.com) associated with this device sent an email warning the recipients that the school was going to be toilet papered. - There were also a number of Google searches conducted on the device related to charmin extra soft and the best toilet paper. - Finally, there was also a memo generated containing a target list that included the following names: 1. Lisa 2. Hilary 3. Diane 4.Principal Skinner
KZFX43	Yes
L66WV3	yes
L6LTN3	Yes
LYLK83	Yes
M3ZEMY	Yes

TABLE 1

Question 38 - Analysis

WebCode	Response
M9L8YY	Yes
MDGY8V	Yes
MHCT6X	yes (This is beyond my scope of expertise)
NDV89V	
NGBFWV	Yes
NUDXH3	Yes, I believe the evidence shows that this device was used to plan the toilet papering of Keys High School. SMS Internet search terms etc. Social Media Email.
PK8DUZ	Yes
QCCWH2	Yes
QQ8CHV	Yes.
QVK6NT	Not generally in the scope of our analysis, but yes
RGCV7W	Yes
RR6VHG	Yes
T8QRYW	Yes
TT8FBU	yes
UFLZ8U	Yes
UQC6QQ	Yes
URBWAT	Yes
V2AL8P	Yes
VHGMPN	Yes
VJC6QP	Yes
VN3F2M	Yes
WWD2MW	Yes
XN3Y2V	Yes
YHLTAN	YES
ZKATLG	Yes
ZVTJVL	yes
ZWTAEN	yes

TABLE 1

Question 38 - Analysis

Consensus Result: Yes

Expected Response Explanation:

This device was used to plan the toilet papering at Keys High School. The following list is a compilation of messages between Stella Frost and Mr. Black from various applications planning the toilet papering and the keywords search found in the internet history:

Tumblr messages:
\data\com.tumblr\databases\tumblr.sqlite

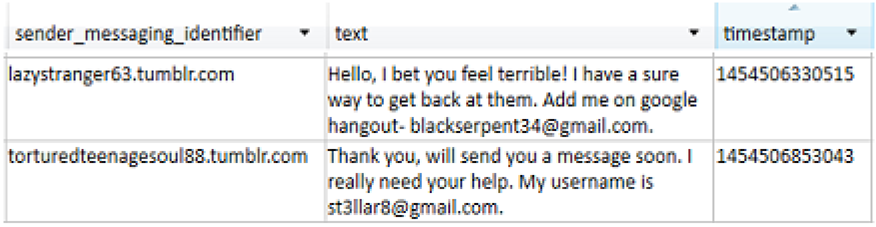
Google Hangouts:
\data\com.google.android.talk\data\babel1.db

Search terms found on the device via Google Chrome:
\data\com.android.chrome\default\history.db

Skype messages:
\data\com.skype.raider\files\frosty.queen12\main.db

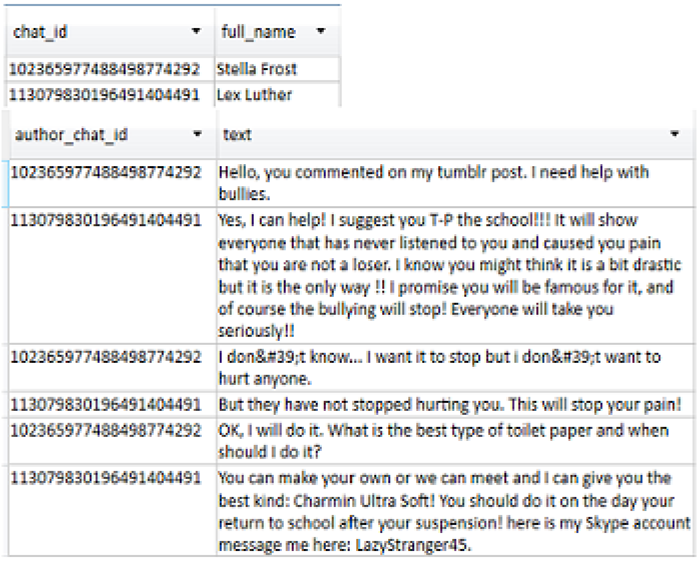
Expected Response Illustration:

Database: tumblr.sqlite >>> Table: messages



sender_messaging_identifier	text	timestamp
lazystranger63.tumblr.com	Hello, I bet you feel terrible! I have a sure way to get back at them. Add me on google hangout- blackserpent34@gmail.com.	1454506330515
torturedteenagesoul88.tumblr.com	Thank you, will send you a message soon. I really need your help. My username is st3llar8@gmail.com.	1454506853043

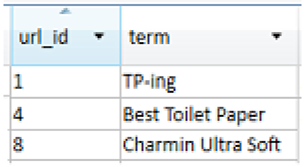
Database: babel1 >>> Table: messages



chat_id	full_name
102365977488498774292	Stella Frost
113079830196491404491	Lex Luther

author_chat_id	text
102365977488498774292	Hello, you commented on my tumblr post. I need help with bullies.
113079830196491404491	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
102365977488498774292	I don&#39;t know... I want it to stop but i don&#39;t want to hurt anyone.
113079830196491404491	But they have not stopped hurting you. This will stop your pain!
102365977488498774292	OK, I will do it. What is the best type of toilet paper and when should I do it?
113079830196491404491	You can make your own or we can meet and I can give you the best kind: Charmin Ultra Soft! You should do it on the day your return to school after your suspension! here is my Skype account message me here: LazyStranger45.

Database: history >>> Table: keyword_search_terms

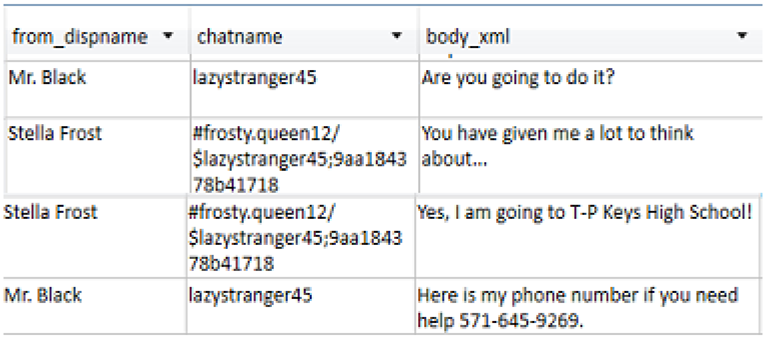


url_id	term
1	TP-ing
4	Best Toilet Paper
8	Charmin Ultra Soft

TABLE 1

Question 38 - Analysis

Database: main >>> Table: messages



from_dispname	chatname	body_xml
Mr. Black	lazystranger45	Are you going to do it?
Stella Frost	#frosty.queen12/ $lazystranger45;9aa1843 78b41718	You have given me a lot to think about...
Stella Frost	#frosty.queen12/ $lazystranger45;9aa1843 78b41718	Yes, I am going to T-P Keys High School!
Mr. Black	lazystranger45	Here is my phone number if you need help 571-645-9269.

TABLE 1

Question 39 - Analysis

Question 39: From your analysis was this device used to make the threat to Keys High School?

Manufacturer's Expected Response: Yes

WebCode	Response
2EKP2R	yes
2L4XFF	Yes
2T3MWK	Yes. E-mails were found including threats to the School.
2ZYCPH	Yes
3XNA9L	SMS ‘already called Keys to make the threat’. Outgoing calls to Keys school
4EAWZL	Yes
67DGNM	Yes. The device was used to call Keys High School and send threatening emails to school officials.
6B4QXK	Possibly. There is a SMS message to Mr. Black saying that a threat call has been done and also Keys High School was called (by phone) about 15 minutes before that SMS message.
6FZH7G	Yes
6JJAHK	Yes
6KETJL	Yes
76HXLK	Yes
77PFKG	Yes
7BNU7K	Yes
7K8NDH	Yes. There is an SMS message sent from this device to '5716459269' on 04/02/2016 which says the threat has been made to Keys. There are two phone calls made from this device to Keys High School on 04/02/2016, the first which was answered was made 18 minutes before the message was sent.
8BHWAF	Yes
8DP7RD	yes
9AEBRE	yes
9CPE9B	Yes
A2MFXG	Yes
AWRL2F	Yes
AZRXWF	Yes
B4BFFC	Yes, from my analysis this device was used to make threats to Keys High School via phone calls and e-mails.
BX4PD7	Yes
C3CNWB	Yes
C9GBYC	Yes. The data--such as call log, e-mails and SMS text messages--found on the submitted image file suggest this device may have been used to make threats to Keys High School.
D37Q26	Yes
D8L2EA	Based on analysis there does appear to have been a threat made to Keys High School from this device. The date associated with the data on the device shows a threat on 04-February-2016.
DHJ3QD	Yes on 2/4/2016 there are 4 phone calls made to Keys High school and the user states in a text message that the threat was made.
DJFH4A	Yes

TABLE 1

Question 39 - Analysis

WebCode	Response
DRKPJA	Yes
E3HPVE	Yes
EG36YD	Yes
EMVHN9	Yes, an email contained a threat message to the school was recovered.
FWP664	No
FXKN86	Yes, Because some messages were found via e-mail. "To Whom It May Concern, On 2/4/2016 there will be a T-Ping of the school! You have been warned!" and found some message via Skype Chat "Yes, I am going to T-P Keys High School!" and event record in calendar about "T-Day"
G63GVA	Yes, There was an e-mail sent stating on 2/4/2016 there will be a T-Ping of the school! you have been warned!
GKUDX6	yes
GNTPT6	Yes
GQNYD8	Yes
GRQTE7	yes
JZ4RHZ	Yes, this device sent emails using the Yahoo account and made phone calls to the school about the threat.
K7GAZZ	Yes
KGL8Y2	Yes
KJ6YQY	Yes
KJNZ38	Yes
KNHWRY	Yes
KUA4A8	YES, based on my analysis of this evidence, I have determined that this device was used to make the threat to Key High School based on the following: - FOUR (4) phone calls were placed to the school - A yahoo email account (notyouraveragejoe78@yahoo.com) associated with this device sent an email warning the recipients that the school was going to be toilet papered. - Finally, there was also a memo generated containing a target list that included the following names: 1. Lisa 2. Hilary 3. Diane 4.Principal Skinner
KZFX43	Yes
L66WV3	yes
L6LTN3	Yes
LYLK83	Yes
M3ZEMY	Yes
M9L8YY	No
MDGY8V	Yes there were multiple messages sent from this device outlining the plans to Toilet Paper the school.
MHCT6X	yes (This is beyond my scope of expertise)
NDV89V	
NGBFWV	Yes
NUDXH3	Email evidence suggest that this phone was used to make a threat to Keys High School. The email from account St3llar8@gmail.com "to whom it may concern, on 2/4/2016 there will be a T-Ping of the school, You have been warned" Subject "Keys" Also SMS "already called Keys to make threat"
PK8DUZ	Yes, Stella (victim) planned to TP the school to stop the bullying.

TABLE 1

Question 39 - Analysis

WebCode	Response
QCCWH2	Yes
QQ8CHV	Yes
QVK6NT	Not generally in the scope of our analysis, but yes
RGCV7W	Yes
RR6VHG	Yes
T8QRYW	Yes
TT8FBU	yes
UFLZ8U	Yes
UQC6QQ	Yes
URBWAT	Yes
V2AL8P	Yes
VHGMPN	Yes
VJC6QP	Yes
VN3F2M	Yes
WWD2MW	Yes
XN3Y2V	Yes
YHLTAN	YES
ZKATLG	Yes
ZVTJVL	yes
ZWTAEN	yes

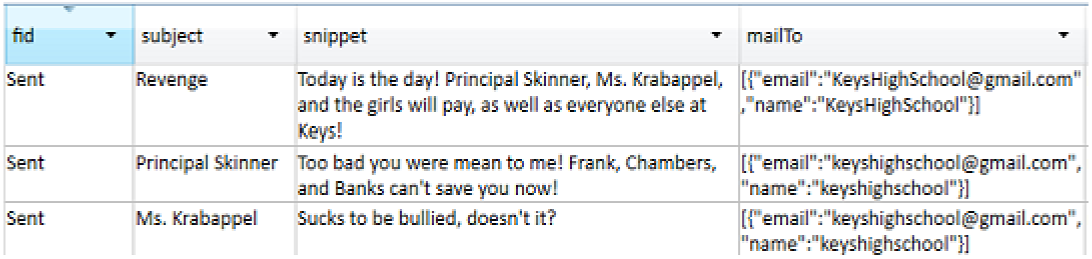
Consensus Result: Yes

Expected Response Explanation:

The information for the direct threats can be found in the e-mails sent to Keys High School via Yahoo E-mail. The messages table shows three e-mails sent to Keys High School. The e-mails can can be found at: \data\com.android.browser\app_ace\databases\https_m.mg.mail.yahoo.com_0\1.db

Expected Response Illustration:

Database: 1 >>> Table: messages



fid	subject	snippet	mailTo
Sent	Revenge	Today is the day! Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!	[{"email":"KeysHighSchool@gmail.com","name":"KeysHighSchool"}]
Sent	Principal Skinner	Too bad you were mean to me! Frank, Chambers, and Banks can't save you now!	[{"email":"keyshighschool@gmail.com","name":"keyshighschool"}]
Sent	Ms. Krabappel	Sucks to be bullied, doesn't it?	[{"email":"keyshighschool@gmail.com","name":"keyshighschool"}]

TABLE 1

Question 40 - Analysis

Question 40: Was a list of targets found? If so, what names were on the list? (Provide real names)

Manufacturer's Expected Response: Yes
Lisa
Hilary
Diane
Principal Skinner
Ms. Krabappel

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
2EKP2R	in yahoo email a sent message was found: "Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!" I believe this is the list of targets
2L4XFF	Principal Skinner, Ms. Krabappel, Diane Chambers, Hilary Banks, Lisa Frank
2T3MWK	Lisa, Hilary, Diane, Principal Skinner, Ms. Krabappel
2ZYCPH	Principal Skinner, Ms Krabappel, "the girls" Lisa Frank, Diane Chambers and Hilary Banks and "everyone else"
3XNA9L	Yes in memo. Lisa Hilary Diane Principal Skinner Ms. Krabappel
4EAWZL	Assuming names in contact book are real, then Lisa Frank, Hilary Banks, Dianne Chambers, Principal Skinner, Ms. Krabappel
67DGNM	The device was used to send threatening emails (notyouraveragejoe28@yahoo.com) specifically naming the following targets: Principal Skinner, Ms. Krabappel, Lisa Frank, Diane Chambers, Hilary Banks and less specifically the rest of Keys High School
6B4QXK	Yes. Targets: Lisa, Hilary, Diane, Principal Skinner, Ms. Krabappel
6FZH7G	Yes. Lisa, Hilary, Diane, Principal Skinner and Ms. Krabappel.
6JJAHK	Yes. Principal Skinner, Ms. Krabappel, Frank (Lisa), Chambers (Diane) and Banks (Hilary)
6KETJL	Principal Skinner Ms. Krabappel The girls: Lisa Frank, Diane Chambers and Hilary Banks
76HXLK	Lisa Frank Hilary Banks Diane Chambers Principal Skinner Ms. Krabappel
77PFKG	Lisa, Hilary, Diane, Principal Skinner and Ms. Krabappel
7BNU7K	Lisa Frank Hilary Banks Diane Chambers Principal Skinner Ms. Krabappel
7K8NDH	Principal Skinner Ms. Krabappel Lisa Hilary Diane
8BHWAF	Principal Skinner Ms. Krabappel Lisa Frank Diana Chambers Hilary Banks
8DP7RD	No list recovered.
9AEBRE	yes. Lisa, Hilary, Diane, Principal Skinner, Ms Krabappel
9CPE9B	Yes. Diane Chambers; Lisa Frank; Hilary Banks.
A2MFXG	No
AWRL2F	No
AZRXWF	Yes in Yahoo email which states Principal Skinner, Ms. Krabapple, and the girls will pay, as well as everyone else at Keys. An additional email to Principal Skinner stating that "Frank, Chambers, and Banks can't save you now!"
B4BFFC	A specific list was not found, but a sent message with the subject "Revenge" stated the following: "Today is the day! Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!" From this, it was inferred that Keys High School was a target, in addition to the following: Principal Skinner, Ms. Krabappel, and "the girls". "The girls" that the person of interest was referring to were most likely: Lisa Frank, Diane Chambers, and Hilary Banks. These three (3) names were inferred from the various emails and chats found in the acquired data from the phone.

TABLE 1

Question 40 - Analysis

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
BX4PD7	A list was not located however based on my analysis, the suspension not contained three names: Hilary Banks, Diane Chambers, and Lisa Frank who are potentially the "targets".
C3CNWB	Yes Principal Skinner, Ms. Krabappel, and the girls (Hilary Banks, Diane Chambers Lisa Frank)
C9GBYC	Yes. "Principal Skinner, Ms. Krabappel, and the girls" were listed as targets in an e-mail. The names of the girls targeted were not specifically given but may be deduced from call log, e-mail, SMS text messages and third-party application chat threads to be Diane Chambers, Hilary Banks and Lisa Frank.
D37Q26	Yes Lisa, Hilary, Diane, Principal Skinner, Ms. Krabappel
D8L2EA	Yes Principal Skinner, Ms. Krabappel, Lisa Frank, Hilary Banks and Diane Chambers Principal Skinner and Ms. Karabappel were specifically mentioned in an email message from “notyouraveragejoe78@yahoo.com” to “keyshighschool@gmail.com”. In the email message “the girls” are mentioned as being among those who will pay. The examiner used previously obtained information from a suspension slip identifying Lisa Frank, Hilary Banks and Diane Chambers as those accused of bullying Stella Frost. Additionally there are messages from contacts matching those names that appear to contain bullying content.
DHJ3QD	no
DJFH4A	Principal Skinner and Mrs. Krabappel
DRKPJA	Lisa Frank Principle Skinner Ms. Krabappel Hilary Banks Diane Chambers
E3HPVE	There was no list found. But the target was Keys High School. There were three individuals that were harassing Stella Frost. There names are: Lisa Frank, Hilary Banks, and Diane Chambers.
EG36YD	Principal Skinner, Mrs. Crabapple, Daine Chambers, Lisa Frank, Hillary Banks
EMVHN9	There wasn’t a direct list of names found, but there were emails found in the Yahoo email account database that targets multiple people. The people targeted were Principal Skinner, Ms. Krabappel, “the girls”, and “everyone else at Keys!” listed in the emails.
FWP664	Lisa Frank, Banks Hilary, Chambers Diane
FXKN86	"Hilary Banks", "Diane Chambers" and "Lisa Frank"
G63GVA	A failed message to keyshighschool@gmail.com listed Principal Skinner, Ms. Krabappel and the girls will pay. Also in a message to frokeyshighschool@gmial.com listed Frank, Chambers, and Banks.
GKUDX6	yes Hilary Banks, Lisa Frank and Diane Chambers
GNTPT6	Diane Chambers Hilary Banks Lisa Frank
GQNYD8	Yes Lisa (Lisa Franks), Hilary (Hilary Banks), Diane (Diane Chambers), Principal Skinner, Ms. Krabappel
GRQTE7	No
JZ4RHZ	Yes, Principal Skinner, Ms. Krabappel, Lisa Frank, Diane Chambers, and Hilary Banks
K7GAZZ	No
KGL8Y2	No list was found but a target was mentioned in the data recovered from the device. Algonkian Park appears to be a meetup location prior to the T-Ping. This does not appear to be a 'target', but there may be security video at the park that may be of evidentiary value.
KJ6YQY	YES. Ms. Krabappel, Lisa Frank, Hilary Banks, Diane Chambers.
KJNZ38	Yes. Lisa, Hillary, Diane, Principal Skinner, Krabappel
KNHWRY	Yes, Principal Skinner, Ms. Krabappel, Hilary, Lisa, Diane
KUA4A8	YES, there was a memo that contained targets, which were as follows: - TARGETS: Lisa Hilary Diane Principal Skinner
KZFX43	Lisa, Hilary, Diane, Principal Skinner, Ms Krabappel
L66WV3	Lisa, Hilary, Diane, Principal Skinner, Ms. Krabappel

TABLE 1

Question 40 - Analysis

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
L6LTN3	Yes: Lisa Hilary Diane Principal Skinner Ms. Krabappel
LYLK83	Yes. Ms. Krabappel, Principle Skinner, Lisa Frank, Hilary Banks, and Diane Chambers
M3ZEMY	There was a message sent with the subject "Revenge" that stated "Today is the day!Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!" The following names were listed in the above mentioned message: Principal Skinner Ms. Krabappel "the girls" The specific names of "the girls" were not mentioned in this particular message. However, another message with the subject "Principal Skinner" was located that stated "Too bad you were mean to me! Frank, Chambers, and Banks can't save you now!". The above mentioned names of Frank, Chambers, and Banks were located in the Contacts as: Lisa Frank Hilary Banks Diane Chambers The above mentioned names appear to be targets of the incident.
M9L8YY	Yes Lisa Frank Hilary Banks Diane Chambers
MDGY8V	Lisa, Hilary, Diane, Principal Skinner, and Ms Krabappel
MHCT6X	Yes Diane Chambers Hilary Banks Lisa Frank Principal Skinner Ms. Krabappel (This is beyond my scope of expertise)
NDV89V	
NGBFWV	Lisa Frank, Hilary Banks, Diane Chambers, Principal Skinner, Ms. Krabappel
NUDXH3	Chat- "Yes, I am going to T-P Keys High School" 2/3/2016 11:57:23 am" also several images depict the toilet papering of the school. and a calendar event "T-day Keys High School"
PK8DUZ	Keys High School Stella Frost
QCCWH2	Yes, "Principal Skinner, Ms Krabappel and the girls"
QQ8CHV	Yes, Lisa Frank, Hilary Banks, Diane Chambers, Principal Skinner, Ms. Krabappel
QVK6NT	From Yahoo Email: Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone at Keys!
RGCV7W	Yes, "Today is the day! Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys! "
RR6VHG	Yes, in mail messages: 1-Lisa Frank, 2-Diana Chambers 3-Hilary Banks 4-Principal Skinner 5-Ms.Krabappel
T8QRYW	Yes. Principle Skinner, Ms. Krabappel , Lisa Frank, Diane Chambers and Hilary Banks.
TT8FBU	Lisa Frank,Hillary Banks, Diane Chambers
UFLZ8U	Hilary Banks, Diane Chambers, Lisa Frank, Principal Skinner, and Ms. Krabappel
UQC6QQ	Principal Skinner and Mrs. Krabappel
URBWAT	In an email with the subject of "Revenge" that was sent to Keys High School, the names of Principle Skinner, Ms. Krabappel, and "the girls" are listed as individuals who "will pay", along with others at Keys, the high school. The girls being referenced are possibly Lisa Frank, Hilary Banks, and Diane Chambers, based off of other emails and messages, where those girls are involved with the device user.
V2AL8P	No
VHGMPN	Yes – Lisa Frank, Hilary Banks, Diane Chambers, Principal Skinner, Ms. Krabappel
VJC6QP	Yes Lisa Hilary Diane Principal Skinner Ms. Krabappel
VN3F2M	Yes Lisa Hilary Diane Principal Skinner Ms. Krabappel
WWD2MW	Yes Lisa Frank Diane Chambers Hillary Banks
XN3Y2V	None found
YHLTAN	yes ,Keys High School

TABLE 1

Question 40 - Analysis

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
ZKATLG	No list found. Possible targets: Keys High School, Diane Chambers, Hilary Banks
ZVTJVL	Nickname: Hilary Banks Nickname: Diane Chambers
ZWTAEN	No specific list was found, however based upon examination, victims could include Diane Chambers, Lisa Frank, Hillary Banks, and Keys High School.

Consensus Result: ** No consensus achieved; Inconsistencies not highlighted **

Expected Response Explanation:

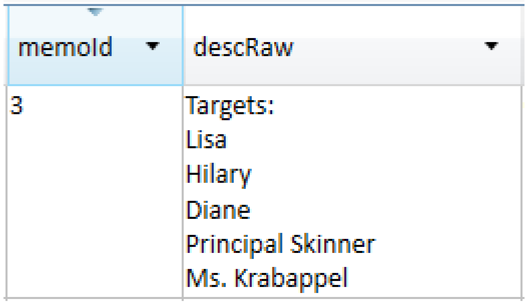
Consensus was not achieved for question 40. A majority of the responses were different variations of the intended list found in the Memo app within the qumemoplus database (Lisa, Hilary, Diane, Principal Skinner, Ms. Krabappel) and the revenge e-mail sent to Keys high School from notyouraveragejoe78@yahoo.com which listed Principal Skinner, Ms. Krabappel, and the girls (Lisa, Hilary, Diane).

This question is asking if a list of targets, such as a hit list, was found on this device and report the names within the list. The Memo application contained three memos: grocery list, music, and targets. The names listed in the targets memo are: Lisa, Hilary, Diane, Principal Skinner, and Ms. Krabappel. Information about memos can be found in the qmemoplus.db database. The memoObject table shows memos created on this device. The file can be found at: \data\com.lge.qmemoplus\databases\qumemoplus.db

Additionally, participants reported one of the threatening e-mails as the list of targets sent to Keys High School from notyouraveragejoe78@yahoo.com. This message titled "Revenge" states "Today is the day! Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!" Information about the revenge e-mail can be found in the 1 database. The messages table will contain information of e-mails sent. The file can be found at: data\com.android.browser\app_ace\databases\https_m.mg.mail.yahoo.com_0\1.db

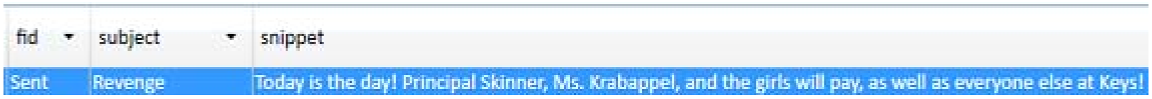
Expected Response Illustration:

Database: qmemoplus >>> Table: memoObject



memoId	descRaw
3	Targets: Lisa Hilary Diane Principal Skinner Ms. Krabappel

Database: 1 >>> Table: messages



fid	subject	snippet
Sent	Revenge	Today is the day! Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!

TABLE 1

Question 41 - Analysis

Question 41: At the conclusion of your analysis of the device are there any persons of interest? (Provide real names)

Manufacturer's Expected Response: Yes
Stella Frost
Lex Luther

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
2EKP2R	Stella Frost- person of interest and apparent owner of the phone Mr. Black- co-conspirator **Note: I would also consider Hillary Banks and Diane Chambers persons of interest because they share an IP address with Mr. Black (info obtained through analysis of Skype data)
2L4XFF	Stella Frost, Mr. Black
2T3MWK	Suspect: Stella Frost. Accessory: Lex Luthor Targets: Lisa Frank, Hilary Banks, Diane Chambers, Principal Skinner, Ms. Krabappel
2ZYCPH	Stella Frost, Mr. Black (Lex Luther)
3XNA9L	Stella Frost, Lex Luther, Mr Black
4EAWZL	Stella Frost Mr. Black
67DGNM	Stella Frost is the primary suspect. Stella Frost is the name used by the owner of the phone used to plan for the toilet papering of Keys High School and communicate the threat to the school. (tourturedteenagesoul88, st3llar8@gmail.com, notyouraveragejoe78@yahoo.com). Additional details for Stella Frost: Student at Keys High School, Suspended 2/1/2016, DOB: 1/7/2000, Image used by Skype account (purple shoe and kitten), Skype location entered as Sterling, us, Metadata on pictures 39.051111, -77.382778 Cascades Pkwy near Algonkian Pkwy Sterling/Potomac Falls Virginia area. MetroPCS/T-Mobile 5714658141. The analysis of the phone revealed that Frost was engaged in a dispute with at least three other girls at Keys High School. Lisa Frank, Hilary Banks, and Diane Chambers. Frost was disciplined after an incident with the girls and felt her treatment by the school was unfair, and the girls continued to bully her. Frost expresses her frustration on social media. Through social media, she begins communicating with a subject using the names Lex Luther and Mr. Black. (blackserpent34@gmail.com, LazyStranger45, and LazyStranger63) This person of interest gives Frost his phone number 571-645-9269 and assists Frost in acquiring the Charmin Ultra Soft for use in the attack on Keys High School.
6B4QXK	Stella Frost and Mr Black alias Lex Luthor (both suspects to a T-P threat)
6FZH7G	Yes. Stella Frost and Lex Luther.
6JJAHK	SUPECTS: Stella Frost Lex Luther – AKA Mr. Black ADDITIONAL PERSONS: Hilary Banks Diane Chambers Lisa Frank Principal Skinner Ms. Krabappel
6KETJL	Stella Frost Lex Luther, aka Mr. Black
76HXLK	Stella Frost and Mr. Black aka Lex Luther
77PFKG	Yes. Lex Luther and Stella Frost
7BNU7K	Stella Frost Mr. Black
7K8NDH	Suspects in Crime: Stella Frost (device user) Lex Luther (third party who helped organise) Mr. Black (third party who helped organise) Others: Lisa Frank (bully/target) Diane Chambers (bully/target) Hilary Banks (bully/target) Principal Skinner (target) Ms. Krabappel (target)
8BHWAF	Lex Luther
8DP7RD	Lex Luther.
9AEBRE	For bullying: Diane Chambers, Hilary Banks, Lisa Frank For Toilet-Papering: Stella Frost, Lex Luther, Mr Black
9CPE9B	Stella frost Lex Luther
A2MFXG	Stella Frost, Diane Chambers, Hilary Banks, Lisa Frank, Mr. Black, Lex Luther

TABLE 1

Question 41 - Analysis

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
AWRL2F	Stella Frost, Lex Luther, Diane Chambers, Hilary Banks, Lisa Frank
AZRXWF	Stella Frost, Mr. Black, Lex Luther
B4BFFC	Stella Frost and Mr. Black (Lex Luther). Although Mr. Black (Lex Luther) did not make direct threats like Stella Frost, he did act as an accomplice in helping Stella Frost plan the T-Ping event at Keys High School.
BX4PD7	Yes. Mr. Black and Stella Frost.
C3CNWB	Mr Black Stella Frost
C9GBYC	Yes. The data--such as device accounts, contacts, call logs, e-mails, SMS text messages and third party application chat threads--found on the submitted image file suggest some persons of interest may be Mr. Black (also known as Lex Luther) and Stella Frost.
D37Q26	Stella Frost, Lex Luther
D8L2EA	Yes Stella Frost, Mr. Black
DHJ3QD	Mr Black should be questioned
DJFH4A	Stella Frost
DRKPJA	Stella Frost Lisa Franks Mr. Black Diane Chambers
E3HPVE	Lex Luther and Stella Frost
EG36YD	Lex Luther
EMVHN9	Yes, Stella Frost and Mr. Black.
FWP664	Stella Frost, Lex Luther
FXKN86	"Stella Frost" and "Lex luther or Mr.Black"
G63GVA	Stella Frost, Lex Luther, Mr. Black
GKUDX6	Principal Skiner Ms Krabappel
GNTPT6	Stella Frost Lex Luther
GQNYD8	Yes Stella Frost Lex Luther
GRQTE7	Diane Chambers Hilary Banks Alexis Ramirez Lisa Frank
JZ4RHZ	Stella Frost – Primary suspect in TP threat to school and individuals Mr. Black (Lex Luther) co-conspirator in TP threat. Possible charges on Lisa Frank, Diane Chambers, and Hilary Banks for cyber bullying depending on current laws.
K7GAZZ	Stella Frost, Lex Luther
KGL8Y2	Yes. Stella Frost, Mr. Black, Lex Luthor
KJ6YQY	Stella Frost, Lex Luther, Ms. Krabappel, Lisa Frank, Hilary Banks, Diane Chambers.
KJNZ38	Stella Frost and Lex Luther
KNHWRY	Lex Luther, Stella Frost

TABLE 1

Question 41 - Analysis

WebCode	Response ** No consensus achieved; Inconsistencies not highlighted **
KUA4A8	YES, based on my analysis of this evidence, STELLA FROST and MR. BLACK should be considered persons of interest. To support my determination, I will specifically point to the following: - Skype communication between frosty.queen12 (STELLA FROST) and lazystranger45 (Mr. Black) pertaining to the toilet papering of the school. Specifically, when the individual using the profile of STELLA FROST told Mr. Black that she was going to T-P Keys High School. - A yahoo email account (notyouraveragejoe78@yahoo.com) associated with this device sent an email warning the recipients that the school was going to be toilet papered. - There were also a number of Google searches conducted on the device related to charmin extra soft and the best toilet paper. - Finally, there was also a memo generated containing a target list that included the following names: 1. Lisa 2. Hilary 3. Diane 4.Principal Skinner
KZFX43	Stella Frost, Lex Luther
L66WV3	stella Frost , lex luther would like to interview stella Frost , Lisa Frank, hillary banks, diane chambers, lex luther
L6LTN3	Stella Frost Lex Luther (Mr. Black)
LYLK83	Stella Frost (suspect),Lex Luther (co-conspirator/accessory)
M3ZEMY	Stella Frost Mr. Black (Lex Luther)
M9L8YY	Lex Luther
MDGY8V	Stella Frost, Mr Black as someone who provided the idea and helped to encourage.
MHCT6X	Stella Frost Lex Luther (This is beyond my scope of expertise)
NDV89V	
NGBFWV	Stella Frost
NUDXH3	I would advised the case agent to conduct interviews and serve possible search warrants on Hilary Banks, Lisa Frank, Diane Chambers. I would advise them to conduct additional field work on acquiring social media accounts etc.
PK8DUZ	Diane Chambers Lisa Frank Hillary Banks Stella Frost Mr. Black
QCCWH2	Stella Frost Lex Luther
QQ8CHV	Lex Luther
QVK6NT	
RGCV7W	Stella Frost, Mr. Black, and Lex Luther
RR6VHG	Lex Luther
T8QRYW	Stella Frost Lex Luther
TT8FBU	Lex Luther, Stella Frost
UFLZ8U	Stella Frost, Lex Luther
UQC6QQ	Stella Frost
URBWAT	Mr. Black (AKA Lex Luther) Stella Frost
V2AL8P	Stella Frost Lex Luther
VHGMPN	Stella Frost, Lex Luther
VJC6QP	Stella Frost Lex Luther
VN3F2M	Stella Frost Lex Luther
WWD2MW	Stella Frost Mr. Banks
XN3Y2V	Stella Frost, Lex Luther
YHLTAN	Lex Luther , Stella Frost ,Diane Chambers

TABLE 1

Question 41 - Analysis

WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
ZKATLG	Stella Frost Mr. Black	
ZVTJVL	Mr. black	
ZWTAEN	Stella Frost Lex Luthor	

Consensus Result: ** No consensus achieved; Inconsistencies not highlighted **

Expected Response Explanation:

Consensus was not achieved for question 41. A majority of the responses were different variations that included Stella Frost and Mr. Black (aka Lex Luther). A minority of the responses included persons of interest for cyber bullying (Lisa Frank, Hilary Banks, Diane Chambers).

Aside from individuals (Lisa Frank, Diane Chambers, and Hiliary Banks) sending harassing messages to this device the only other communication was between Stella Frost and Mr. Black across different applications. These applications include: Tumblr, Google Hangouts, & Skype. Examples of Stella's communications with Mr. Black can be found at the following paths:

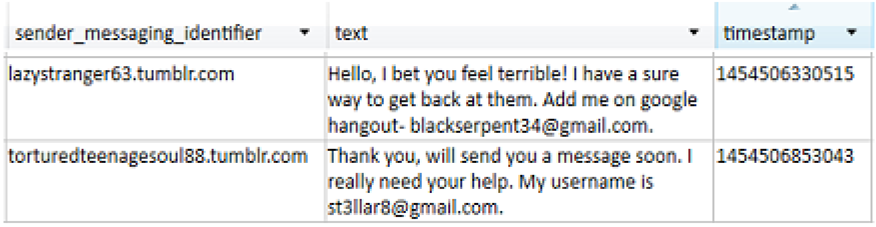
Tumblr messages:
\data\com.tumblr\databases\tumblr.sqlite.db

Google Hangout messages:
\data\com.google.android.talk\data\babel1.db

Skype messages:
\data\com.skype.raider\files\frosty.queen12\main.db

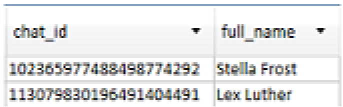
Expected Response Illustration:

Database: tumblr.sqlite >>> Table: messages

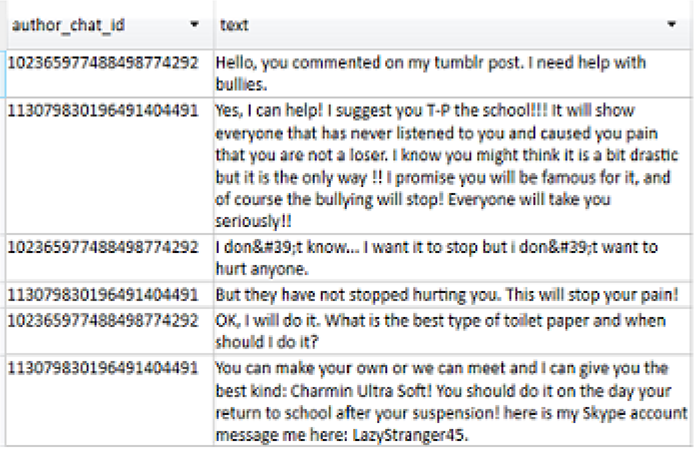


sender_messaging_identifier	text	timestamp
lazystranger63.tumblr.com	Hello, I bet you feel terrible! I have a sure way to get back at them. Add me on google hangout- blackserpent34@gmail.com.	1454506330515
torturedteenagesoul88.tumblr.com	Thank you, will send you a message soon. I really need your help. My username is st3llar8@gmail.com.	1454506853043

Database: babel1 >>> Table: messages



chat_id	full_name
102365977488498774292	Stella Frost
113079830196491404491	Lex Luther

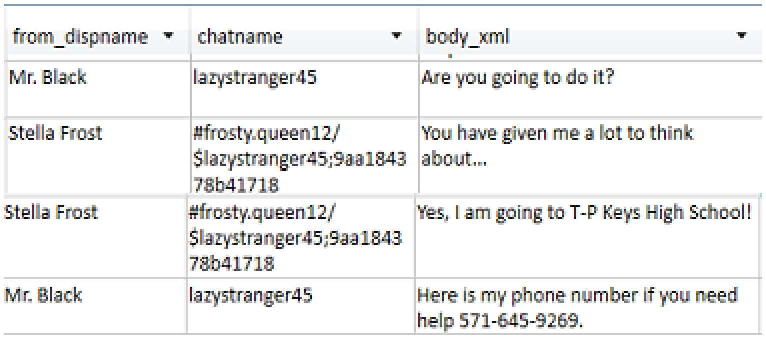


author_chat_id	text
102365977488498774292	Hello, you commented on my tumblr post. I need help with bullies.
113079830196491404491	Yes, I can help! I suggest you T-P the school!!! It will show everyone that has never listened to you and caused you pain that you are not a loser. I know you might think it is a bit drastic but it is the only way !! I promise you will be famous for it, and of course the bullying will stop! Everyone will take you seriously!!
102365977488498774292	I don&#39;t know... I want it to stop but i don&#39;t want to hurt anyone.
113079830196491404491	But they have not stopped hurting you. This will stop your pain!
102365977488498774292	OK, I will do it. What is the best type of toilet paper and when should I do it?
113079830196491404491	You can make your own or we can meet and I can give you the best kind: Charmin Ultra Soft! You should do it on the day your return to school after your suspension! here is my Skype account message me here: LazyStranger45.

TABLE 1

Question 41 - Analysis

Database: main >>> Table: messages



from_dispname	chatname	body_xml
Mr. Black	lazystranger45	Are you going to do it?
Stella Frost	#frosty.queen12/ $lazystranger45;9aa1843 78b41718	You have given me a lot to think about...
Stella Frost	#frosty.queen12/ $lazystranger45;9aa1843 78b41718	Yes, I am going to T-P Keys High School!
Mr. Black	lazystranger45	Here is my phone number if you need help 571-645-9269.

Additional Comments

TABLE 2

WebCode	Additional Comments
2EKP2R	I think this test is pretty in-depth. I enjoyed the challenge however I thought some of the way the questions were worded were a bit vague, leaving me to wonder if I had the answer you were looking for. For instance- the question regarding wireless networks: it appeared that the only network with 'actual data' was Google Starbucks, however there were multiple other instances of other networks with example and test data. I was left wondering if those were to be treated as involved in the scenario, or if they didn't count. Also the Skype data had some sharing of IP data- so I wasn't sure if that was simply a part of creating the test scenario, or if that was an actual investigative conclusion I was supposed to make.
3XNA9L	Tools used; UFED physical analyzer, IEF.
4EAWZL	Question 19 is too ambiguous, many interfaces/apps use as back end the google search engine. Hence, the search results from the chrome app and the android browser are included in the answer. Since they also use the google search engine.
67DGNM	A report was created with supporting data relating to the case for further review by the case agent. Tools: Cyohash Internet Evidence Finder 6.7.8.1853 Forensic Explorer 3.5.7 Physical Analyzer 5.0.2.10 DB Browser for SQLite: 3.8.8.2
6B4QXK	Scenario: “January 21, 2016” is apparently wrong? Scenario: “… Keys High School received toilet papering threats against Keys High School”. In reference to question 39, it would have been nice to know what channel (phone call, instant message, anonymous letter) was used, its details and time of the threat. Question 40: What does “real names” mean? If a name is found on a target list, why should I, as a technical investigator, guess what her/his “real name” is? Question 41: What does “persons of interest” mean? Suspects, victims, threatened persons, anybody?
6KETJL	Question 40: The email reads: "Today is the day! Principal Skinner, Ms. Krabappel, and the girls will pay, as well as everyone else at Keys!" Unable to provide a real name for "everyone else at Keys"
8DP7RD	other evidence was located on this phone including: images of a building with TP in front of it. images of Charmin TP.
AZRXWF	Evidence of bullying in the chats area on Physical Analyzer, Evidence in the chats also indicates that at 02/03/16 at 4:57PM UTC Stella Frost stated "Yes, I am going to T-P Keys High School. Several images of T-P and T-Ping events were located in the image. A picture was taken with the device of a drawing of a building with "Keys H. S." displayed on the building and a roll of toilet paper under the building.
B4BFFC	Information in parentheses following response/answer, (i.e. (userdata(ExtX)/Root/misc/bluedroid/bt_config.xml)) contains the location/file where response/answer was found.
BX4PD7	Based on the analysis of the device, Stella Frost is the owner of the device. She was being bullied by Diane Chambers, Lisa Frank, and Hilary Banks. Their names were found listed on a suspension notice from the school principal. The comment states that Stella reported the names mentioned above as bullying her. Further analysis of the phone shows chats and emails from the three individuals where they are threatening physical harm and insulting Stella. Stella appeared to post her issue on Tumblr and Mr. Black made contact after seeing the post. Mr. Black appears to have several aliases/user accounts. The account names

TABLE 2

WebCode	Additional Comments
	LazyStranger63, blackserpent34, and LazyStranger45 are all tied together with the contact Mr. Black. Mr. Black discusses the idea of TP-ing the school to teach everyone a lesson. Ms. Frost appears reluctant at first, stating she didn't want to harm anyone but then appears to make up her mind to TP the school. Text messages to and from contact, Mr. Black, discuss a pick up point for the Charmin toilet paper. Based on the information on this device, further investigation into Mr. Frank and Stella Frost is necessary.
D8L2EA	Question 5: The location provided by these database fields is Dulles Town Center, Virginia. However, this isn't an actual city in Virginia. After performing a Google search, Dulles Town Center is found to be a mall with several different addresses associated with it Dulles Town Center, Potomac, Virginia Dulles Town Center, 2110 Dulles Town Circle, Dulles, Virginia Dulles Town Center, Dulles Town Circle, Sterling, Virginia All of these city/town locations overlap based on the way Virginia establishes its borders. One is a census-based area, one is an unincorporated area, etc. Question 26: This question is subjective in its identification and linking of usernames based on such limited information and borders on investigation rather than examination. Question 28: The wording of this question does not ask for the number of the contact listed as Keys High School. This creates an issue if the examiner follows up through additional searching and finds that the number for Keys High School is actually the number for CTS Testing. Question 32: The username in the question is listed as "tourturedteenagesoul88". The actual username in the tumblr database and on the tumblr website is "torturedteenagesoul88". So in essence there is no answer to this question if the examiner interprets the username literally. Questions 37-40: These questions are subjective answers of an investigative nature. Of most concern is question 40 because there is no actual list of targets and this information is compiled from various sources including emails and the suspension slip. But this information is deductive reasoning based and not based on an actual list of targets as is asked in the question.
DHJ3QD	additional web searches and images of TP were found as well.
DJFH4A	There is no record of bluetooth connections. There also were no voicemails left on the device.
FXKN86	Confused with your scenario timeline. T-Ping occurred on January 21, 2016 and you did not let me know that when did police found the phone (in the beginning understand that evidence was seized on January 21, 2016 but from physical data found some information after that day. When did police seized the phone January 21, 2016 or February 4, 2016.????????
GQNYD8	We didn't know how flexible we could be with our answers, especially for analysis questions that require more detailed reasoning. We didn't know if we could put in where we got our answers. We decided to answer very succinctly. For date/time format with UTC offset, I was unsure how strictly the format was going to be graded. (e.g. is "02-January-2016; 12:34:56-5" and "02-January-2016; 12:34:56 UTC-5" both okay?) Perhaps in the future, providing a concrete example will help clarify this. We wanted to print our answers. On Chrome, printing skipped questions #21 and #36 by default. #36: How many e-mails were sent using Yahoo account? Answer can be 3 or 6. In the database /data/com.android.browser/app_ace/databases/https_m.mg.mail.yahoo.com_0/1, the 'messages' table showed 3 messages with 'fid' column as "Sent". But the 'folder' table for 'Sent' row with 'total' column shows 6. The test was fair but quite difficult if one has never gone deep into the required databases before. More difficult than other computer exams. A bit too difficult. It was very time-consuming to double-check the answers.

TABLE 2

WebCode	Additional Comments
JZ4RHZ	Test has improved on focus of format and expected answer. Although, there are still a few questions that leave interpretation of a question with multiple possible answers.
KGL8Y2	I am sure it is hard to word questions in such a way that alleviates all questions a test subject might have. As this is my first test, i'm sure I'll get used to the way questions are asked here. i hope there is some feedback on the questions to see which ones, if any, were missed.
KUA4A8	The raw image could not be processed or viewed with any of the mobile forensic tools that are utilized within our laboratory, therefore the majority of the analysis required the use of free, open-source database viewers/readers, as well as EnCase.
MDGY8V	Question 3: What is the device name as reported in the android provider's settings? There were multiple possible answers on this one. Again multiple databases on this answer 5: As per the LGE weather settings, which city/state is set as the location? (ANSWER MUST BE PRESENTED AS "City, State") Answer: Dulles Town Center, Virgina Question 40: Was a list of targets found? If so, what names were on the list? (Provide real names) Answer: Lisa, Hilary, Diane, Principal Skinner, and Ms Krabappel Please be more specific if you want first name last name it just says real name that could be just first name or could be full name.
NDV89V	[Participant reported "This service is not provided" for questions 38, 39, 40, 41.]
NUDXH3	I would encourage encourage the case agent to follow up on leads provided by the analysis of the suspect device.
QQ8CHV	No. It was a nice test
QVK6NT	[Participant reported "Not in the scope of our analysis" for question 41.]
RR6VHG	A student named Stella Frost (cell phone owner) in the school is under pressure(bullying) like she is fat, noone loves her from his school mates,Lisa Frank,Diana Chambers,Hilary Banks. But she gets suspension punishment. For this case she wants to revenge and get in touch with Lex Luther(Mr Black) by Tumblr (Lex Luther comments about her post) and they share their hangout accounts. Lex Luther sends hangout messages and suggets her some ways to make TPing planning. By Skype message Lex Luther asks her what she did and she says she would do. She sends TP warning email to herself(notyouravaragejoe78@yahoo.com) and then sends threat messages to the school's mail adresses.
UQC6QQ	There was no record of Bluetooth devices connected to this device. There were no record of voicemails on this device.
VN3F2M	Regarding Time formats: It is unclear if the hours are being asked for in 24 or 12 hour format. The "HH" suggests military time and thus why I entered them as such. This is far too time intensive. If the object is to see if we can parse out information in databases or within hexadecimal, there could be fewer questions and more focus.