Collaborative Testing Services, Inc
FORENSIC TESTING PROGRAM

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

Mobile Digital Evidence
Test No. 19-5550 Summary Report

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 62 participants 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.

Manufacturer's Information

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

SAMPLE PREPARATION:
A scripted scenario, based upon a drug trafficking case was created to generate user data on the evidence Android device. The execution of the scripted crime took place the week of November 26, 2018. A Samsung J7 Sky Pro smart phone was used to perform the activities and generate the intended artifacts.

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

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

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

SCENARIO PROVIDED TO PARTICIPANTS

Police are investigating a drug trafficking case. They seized approximately 40 grams of cocaine from an abandoned car near Olde Izaak Walton Park. Along with other things, police found a Galaxy J7 phone in the abandoned vehicle. The smart phone was seized and logged as evidence. A physical image of the evidence device was created and you have been tasked with analyzing the physical image utilizing your own tools and methods to determine if it has any information which could assist police with the investigation.

Manufacturer's Information, continued

Question	Manufacturer's Expected Response
1	Provide the MD5 hash value for the decompressed image file. *48bc55857b2a2513dec564d6d889caa2*
2	Provide the SHA1 (base 16) hash value for the decompressed image file. *c9630a98916b129b57c27a421cfd42b315fd89ee*
3	Based on your analysis, was location service enabled on the device? Yes/No *Yes*
4	What is the set time zone for this device? Provide your answer in the following format: City/Country *New York/America*
5	What is the 15 digit International Mobile Subscriber Identity (IMSI) number associated with the device? *311480373589089*
6	Provide the MAC address of the device. *DC:74:A8:DA:F5:0D*
7	When was the SIM activated/changed on this device? Provide the answer in UNIX epoch time. Do not round the value. Answer must include milliseconds. *1542820248368*
8	Provide the operating system (OS) version installed on the device. *6.0.1*
9**	As per the Bluetooth configuration file, this device was connected to a vehicle. Provide the bluetooth name to which this device was connected to last. *HandsFreeLink*
10	Provide the date and time of when this device was last turned on. Answer using the time zone set on the device using the following format: Month/Date/Year Hour:Minutes AM/PM *12/3/2018 08:19 AM*
11	How many wireless networks was this device connected to? *Three (3)*
12	What is the most used 5 digit Location Area Code (LAC) by this device? *29953*
13	What is the Google e-mail account associated with this device? *diazcarlos1185@gmail.com*

Manufacturer's Information, continued

Question	Manufacturer's Expected Response
14	In a travel inquiry email sent to "travel@travelharmony.com" on 11/28/2018 at 10:28 AM(UTC-5), what was the requested destination? Provide the name of the destination only, not the complete email. *Bermuda*
15	Provide the subject of the email associated with Message ID "16184799431074416 24" and Conversation ID "1618479909836767520". *Meeting Location*
16	Provide the names of all the drugs listed in the email received on 1543511979025. Separate the answer using a comma (,) *Marijuana, Heroin, cocaine*
17	Provide the epoch timestamp of the last email sent to John Fuller at "Johnfuller82@yahoo.com". Do not round the value. Answer must include milliseconds. *1543513804000*
18	What was the last term searched using the Mozilla Firefox search engine? *grams to ounce conversion*
19	How many PDF documents were downloaded using the Chrome search engine? *Two (2)*
20	How many pages were bookmarked on the Chrome search engine? *Two (2)*
21**	Provide the names of two pictures which were deleted. Separate answer with a comma(,) *K2-Spice.jpg, Tattoo-design-7.jpg*
22	How many pictures were taken using this camera? Do not include screenshots and downloads. *Two (2)*
23	What is the phone number of contact named "John Fuller"? Answer using the following format: 000-000-0000 *703-544-6952*
24**	Provide the epoch timestamp value of the last phone call placed to 703-544-6952. *1543424651904*
25	To what phone number was the LAST call placed (outgoing) using this device? Provide the phone number in the following format: 000-000-0000 *407-671-0983*
26**	How many outgoing calls were placed from this device? Do not include deleted calls. *Five (5)*

Manufacturer's Information, continued

Question	Manufacturer's Expected Response
27	Provide the last term searched using Google Play Store. *telegram*
28	A calendar event was scheduled with a start date and time of 1544486400000. Provide the subject of the meeting. *Shipment Pickup*
29	What is John Fuller's user ID (Party identifier) for the Telegram application? *706302018*
30	Based on the conversation on the Telegram application, provide the name of the new supplier. (First Last) *Joe Monzo*
31	What is the version of the Telegram Application that is installed on this device? *4.9.1*
32	What is the package_name for the Whisper Application? *sh.whisper*
33	Provide the date of when the Whisper Application was downloaded (purchased)? Answer using the time zone set on the device using the following format: Month/Date/Year (MM/DD/YYYY) *11/27/2018*
34	Provide the username associated with the Whisper Application? *Trout_wow*
35	Provide the body of the last message sent using the Whisper Application. Do not abbreviate or condense your answer. *Hey Buddy, I am here. Where are you?*
36	Provide the username with whom the user had the most communication via the Whisper Application. *Ice_Junky*
37	Provide the title of the deleted note in the Evernote application. *October Status*
38	Provide the User ID associated with the third party application - 'Keeper Password Manager & Secure Vault'. *diazcarlos1185@gmail.com*
39	Provide the account password associated with the third party application - 'Keeper Password Manager & Secure Vault'. *password85*

Manufacturer's Information, continued

Question	*Manufacturer's Expected Response*
40	Did the User ID found within the 'Keeper Password Manager & Secure Vault' application database match with the User ID stored as notes in the Evernote application? Yes or No *Yes*
41	How many records were saved in the Keeper Application? *Four (4)*
42	Was the Waze application used to travel to 775 Gateway Dr SE, Leesburg, VA 20175? Yes or No *No*
43	Provide the name of the last location this device traveled to using the Waze application. *Olde Izaak Walton Park*

Summary Comments

The purpose of this Mobile Digital Evidence (MDE) Test is to allow participants to evaluate their proficiency in analyzing digital artifacts using their own tools and methods. The participants were provided with a scripted scenario, the data extracted from a smart phone in .BIN and .DD file formats, and a series of questions related to the extracted data. (See Manufacturer's Information for preparation details, test scenario, and test questions)

The participants were requested to analyze various digital artifacts including: image details, phone and network settings, native and third party applications, communications, web browser history, and Geo-Location information.

Of the 43 total questions, four questions did not reach a consensus response. These four questions were found in the following three skill sets: Settings/Features, Media, and Native Applications. In addition, Question 42 had an interesting outcome where only 23% reported the expected response of "No" and the remaining 77% reported "Yes" to the inquiry of whether the Waze application was used to travel to a certain location. This discrepancy could possibly be related to the fact that this particular address had been entered into the application, yet the application was never used to navigate to this location.

Notably, a portion of inconsistent responses across the collection of questions may have been due to typographical errors and others were due to not answering the question in the requested format.

We realize that the Digital Forensics field is increasing in complexity and there are generally not many clearly-defined answers. Similarly for this test, participants should follow their laboratory's policies and procedures when evaluating the MDE proficiency test questions.

Digital Evidence Responses

TABLE 1

Question 1 - Image Details

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

Manufacturer's Expected Response: 48bc55857b2a2513dec564d6d889caa2

WebCode	Response
26L4K9	48BC55857B2A2513DEC564D6D889CAA2
2HT9U9	48BC55857B2A2513DEC564D6D889CAA2
3DTGYG	48bc55857b2a2513dec564d6d889caa2
4DUFQ6	48bc55857b2a2513dec564d6d889caa2
4PYWYP	48bc55857b2a2513dec564d6d889caa2
4WN9JF	48bc55857b2a2513dec564d6d889caa2
4ZJ6ZT	48bc55857b2a2513dec564d6d889caa2
64G4UJ	48bc55857b2a2513dec564d6d889caa2
6MTQHC	48bc55857b2a2513dec564d6d889caa2
6XUBJJ	48BC55857B2A2513DEC564D6D889CAA2
7HDKDP	48bc55857b2a2513dec564d6d889caa2
7Q8P8Q	48bc55857b2a2513dec564d6d889caa2
7XHAQJ	48bc55857b2a2513dec564d6d889caa2
84UA8D	48bc55857b2a2513dec564d6d889caa2
8AWL3B	48bc55857b2a2513dec564d6d889caa2
8Q7ENT	48bc55857b2a2513dec564d6d889caa2 (MDE 19-5550.bin)
9RWZUN	48bc55857b2a2513dec564d6d889caa2
9WB7YB	48BC55857B2A2513DEC564D6D889CAA2
AL337X	48bc55857b2a2513dec564d6d889caa2
APKHAX	48BC55857B2A2513DEC564D6D889CAA2
B83YXC	48BC55857B2A2513DEC564D6D889CAA2
BEHJY4	48BC55857B2A2513DEC564D6D889CAA2
BHZGTL	48bc55857b2a2513dec564d6d889caa2
CAKFT3	48BC55857B2A2513DEC564D6D889CAA2
CRPM96	48BC55857B2A2513DEC564D6D889CAA2
DQMCP7	48bc55857b2a2513dec564d6d889caa2
ETRARM	48bc55857b2a2513dec564d6d889caa2

TABLE 1

Question 1 - Image Details	
WebCode	**Response**
F3CZRJ	48bc55857b2a2513dec564d6d889caa2
FCDKRQ	48bc55857b2a2513dec564d6d889caa2
FFWFVJ	48bc55857b2a2513dec564d6d889caa2
FJHEUY	48bc55857b2a2513dec564d6d889caa2
GBC7GA	48bc55857b2a2513dec564d6d889caa2
GDR6K2	48BC55857B2A2513DEC564D6D889CAA2
GNPA6M	48bc55857b2a2513dec564d6d889caa2
GYL92Y	48BC55857B2A2513DEC564D6D889CAA2
HPXMMN	48bc55857b2a2513dec564d6d889caa2
HXQXXJ	04769E76F05672774F1614995EE03FAD
J69MWJ	008121b0b88f26e12a8dadc8b4b98596
JYHDML	48BC55857B2A2513DEC564D6D889CAA2
KAXHF3	48bc55857b2a2513dec564d6d889caa2
KGEDVW	48BC55857B2A2513DEC564D6D889CAA2
MN787Z	48bc55857b2a2513dec564d6d889caa2
N34LXG	48bc55857b2a2513dec564d6d889caa2
N6PKXX	48bc55857b2a2513dec564d6d889caa2
N9RLXU	48bc55857b2a2513dec564d6d889caa2
NAGYFD	48bc55857b2a2513dec564d6d889caa2
PAWF9K	008121B0B88F26E12A8DADC8B4B98596
RUGWR6	48bc55857b2a2513dec564d6d889caa2
UR36WT	48bc55857b2a2513dec564d6d889caa2
VKGQ9D	48bc55857b2a2513dec564d6d889caa2
VXNLJ4	48bc55857b2a2513dec564d6d889caa2
W94QCK	48bc55857b2a2513dec564d6d889caa2
WAU23D	48BC55857B2A2513DEC564D6D889CAA2
WDTCYD	48BC55857B2A2513DEC564D6D889CAA2
WZ8ZM4	48BC55857B2A2513DEC564D6D889CAA2
X78YBX	48BC55857B2A2513DEC564D6D889CAA2
XV7BJ2	48BC55857B2A2513DEC564D6D889CAA2

TABLE 1

Question 1 - Image Details	
WebCode	**Response**
YMTMH8	48BC55857B2A2513DEC564D6D889CAA2
YUUYE6	48BC55857B2A2513DEC564D6D889CAA2
Z6A48L	48BC55857B2A2513DEC564D6D889CAA2
Z8YEXE	48BC55857B2A2513DEC564D6D889CAA2
ZJRXE7	48BC55857B2A2513DEC564D6D889CAA2

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

Consensus Result: 48bc55857b2a2513dec564d6d889caa2

Expected Response Explanation:

This hash value can be achieved by extracting the sample image file from the provided ZIP folder and running a MD5 hashing algorithm on the file.

Expected Response Illustration:

MD5 Hash Value:

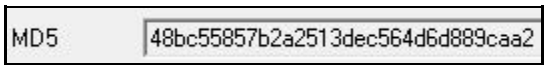


TABLE 1

Question 2 - Image Details

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

Manufacturer's Expected Response: c9630a98916b129b57c27a421cfd42b315fd89ee

WebCode	Response
26L4K9	C9630A98916B129B57C27A421CFD42B315FD89EE
2HT9U9	C9630A98916B129B57C27A421CFD42B315FD89EE
3DTGYG	c9630a98916b129b57c27a421cfd42b315fd89ee
4DUFQ6	c9630a98916b129b57c27a421cfd42b315fd89ee
4PYWYP	c9630a98916b129b57c27a421cfd42b315fd89ee
4WN9JF	c9630a98916b129b57c27a421cfd42b315fd89ee
4ZJ6ZT	c9630a98916b129b57c27a421cfd42b315fd89ee
64G4UJ	C9630a98916b129b57c27a421cfd42b315fd89ee
6MTQHC	c9630a98916b129b57c27a421cfd42b315fd89ee
6XUBJJ	C9630A98916B129B57C27A421CFD42B315FD89EE
7HDKDP	c9630a98916b129b57c27a421cfd42b315fd89ee
7Q8P8Q	c9630a98916b129b57c27a421cfd42b315fd89ee
7XHAQJ	c9630a98916b129b57c27a421cfd42b315fd89ee
84UA8D	c9630a98916b129b57c27a421cfd42b315fd89ee
8AWL3B	c9630a98916b129b57c27a421cfd42b315fd89ee
8Q7ENT	c9630a98916b129b57c27a421cfd42b315fd89ee (MDE 19-5550.bin)
9RWZUN	c9630a98916b129b57c27a421cfd42b315fd89ee
9WB7YB	C9630A98916B129B57C27A421CFD42B315FD89EE
AL337X	c9630a98916b129b57c27a421cfd42b315fd89ee
APKHAX	C9630A98916B129B57C27A421CFD42B315FD89EE
B83YXC	C9630A98916B129B57C27A421CFD42B315FD89EE
BEHJY4	C9630A98916B129B57C27A421CFD42B315FD89EE
BHZGTL	c9630a98916b129b57c27a421cfd42b315fd89ee
CAKFT3	C9630A98916B129B57C27A421CFD42B315FD89EE
CRPM96	C9630A98916B129B57C27A421CFD42B315FD89EE
DQMCP7	c9630a98916b129b57c27a421cfd42b315fd89ee
ETRARM	c9630a98916b129b57c27a421cfd42b315fd89ee
F3CZRJ	c9630a98916b129b57c27a421cfd42b315fd89ee
FCDKRQ	c9630a98916b129b57c27a421cfd42b315fd89ee

TABLE 1

Question 2 - Image Details	
WebCode	**Response**
FFWFVJ	c9630a98916b129b57c27a421cfd42b315fd89ee
FJHEUY	c9630a98916b129b57c27a421cfd42b315fd89ee
GBC7GA	c9630a98916b129b57c27a421cfd42b315fd89ee
GDR6K2	C9630A98916B129B57C27A421CFD42B315FD89EE
GNPA6M	c9630a98916b129b57c27a421cfd42b315fd89ee
GYL92Y	C9630A98916B129B57C27A421CFD42B315FD89EE
HPXMMN	c9630a98916b129b57c27a421cfd42b315fd89ee
HXQXXJ	C64430316C37E614797673C94286EB2D3191334E
J69MWJ	C9630A98916B1295B7C27A421CFD42B315FD89EE
JYHDML	C9630A98916B129B57C27A421CFD42B315FD89EE
KAXHF3	c9630a98916b129b57c27a421cfd42b315fd89ee
KGEDVW	C9630A98916B129B57C27A421CFD42B315FD89EE
MN787Z	c9630a98916b129b57c27a421cfd42b315fd89ee
N34LXG	c9630a98916b129b57c27a421cfd42b315fd89ee
N6PKXX	c9630a98916b129b57c27a421cfd42b315fd89ee
N9RLXU	C9630A98916B129B57C27A421CFD42B315FD89EE
NAGYFD	c9630a98916b129b57c27a421cfd42b315fd89ee
PAWF9K	6A55F3DD5070F0EFAE65A69E249F211744055B2A
RUGWR6	c9630a98916b129b57c27a421cfd42b315fd89ee
UR36WT	c9630a98916b129b57c27a421cfd42b315fd89ee
VKGQ9D	c9630a98916b129b57c27a421cfd42b315fd89ee
VXNLJ4	c9630a98916b129b57c27a421cfd42b315fd89ee
W94QCK	c9630a98916b129b57c27a421cfd42b315fd89ee
WAU23D	C9630A98916B129B57C27A421CFD42B315FD89EE
WDTCYD	C9630A98916B129B57C27A421CFD42B315FD89EE
WZ8ZM4	C9630A98916B129B57C27A421CFD42B315FD89EE
X78YBX	c9630a98916b129b57c27a421cfd42b315fd89ee
XV7BJ2	C9630A98916B129B57C27A421CFD42B315FD89EE
YMTMH8	C9630A98916B129B57C27A421CFD42B315FD89EE
YUUYE6	C9630A98916B129B57C27A421CFD42B315FD89EE

TABLE 1

Question 2 - Image Details	
WebCode	**Response**
Z6A48L	C9630A98916B129B57C27A421CFD42B315FD89EE
Z8YEXE	C9630A98916B129B57C27A421CFD42B315FD89EE
ZJRXE7	C9630A98916B129B57C27A421CFD42B315FD89EE

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

Consensus Result: c9630a98916b129b57c27a421cfd42b315fd89ee

Expected Response Explanation:

This hash value can be achieved by extracting the sample image file from the provided ZIP folder and running a SHA1 hashing algorithm on the file.

Expected Response Illustration:

SHA1 Hash Value:

SHA1	c9630a98916b129b57c27a421cfd42b315fd89ee

TABLE 1

Question 3 - Settings/Features

Question 3: Based on your analysis, was location service enabled on the device? Yes/No

Manufacturer's Expected Response: Yes

WebCode	Response
26L4K9	Yes
2HT9U9	Yes
3DTGYG	Yes
4DUFQ6	Yes
4PYWYP	Yes
4WN9JF	Yes
4ZJ6ZT	Yes
64G4UJ	Yes
6MTQHC	Yes
6XUBJJ	Yes
7HDKDP	Yes
7Q8P8Q	Yes
7XHAQJ	Yes
84UA8D	Yes
8AWL3B	Yes
8Q7ENT	Yes
9RWZUN	Yes
9WB7YB	Yes
AL337X	Yes
APKHAX	Yes
B83YXC	Yes
BEHJY4	Yes
BHZGTL	Yes
CAKFT3	Yes
CRPM96	Yes
DQMCP7	Yes
ETRARM	Yes
F3CZRJ	Yes
FCDKRQ	Yes

TABLE 1

Question 3 - Settings/Features	
WebCode	**Response**
FFWFVJ	Yes
FJHEUY	Yes
GBC7GA	Yes
GDR6K2	Yes
GNPA6M	Yes
GYL92Y	Yes
HPXMMN	Yes
HXQXXJ	Yes
J69MWJ	Yes
JYHDML	Yes
KAXHF3	Yes
KGEDVW	Yes
MN787Z	Yes
N34LXG	Yes
N6PKXX	Yes
N9RLXU	Yes
NAGYFD	Yes
PAWF9K	Yes
RUGWR6	Yes
UR36WT	Yes
VKGQ9D	Yes
VXNLJ4	Yes
W94QCK	Yes
WAU23D	Yes
WDTCYD	Yes
WZ8ZM4	Yes
X78YBX	Yes
XV7BJ2	Yes
YMTMH8	Yes
YUUYE6	Yes

TABLE 1

Question 3 - Settings/Features	
WebCode	**Response**
Z6A48L	Yes
Z8YEXE	Yes
ZJRXE7	Yes

Question 3: Based on your analysis, was location service enabled on the device? Yes/No

Consensus Result: Yes

Expected Response Explanation:

The "googlesetting.db" database stores a record which indicates that the user has opted to allow Google's services access to the device. This database is located at:
/Root/data/com.google.android.gsf/databases/googlesettings.db-wal

Expected Response Illustration:

Location Settings:

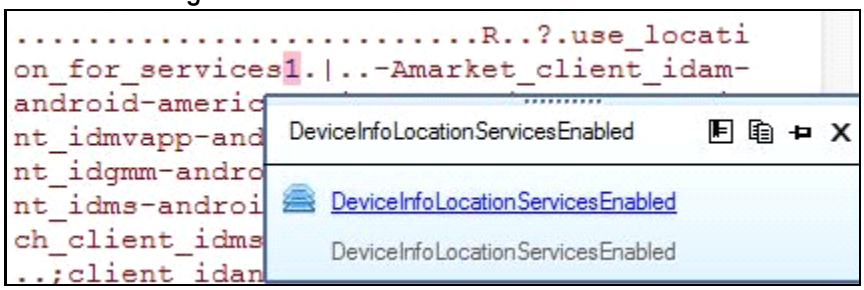


TABLE 1

Question 4 - Settings/Features

Question 4: What is the set time zone for this device? Provide your answer in the following format: City/Country

Manufacturer's Expected Response: New York/America

WebCode	Response
26L4K9	New York/USA
2HT9U9	New York/America
3DTGYG	New York/America
4DUFQ6	New York/America
4PYWYP	New York/America
4WN9JF	New_York/America
4ZJ6ZT	New York/America
64G4UJ	New York/America
6MTQHC	New York/America
6XUBJJ	New_York/America
7HDKDP	New York/America
7Q8P8Q	New York/America
7XHAQJ	New York/America
84UA8D	New York/United States
8AWL3B	New York/America (UTC-05:00)
8Q7ENT	UTC -05:00 New York/America
9RWZUN	New_York (America)
9WB7YB	New York/America
AL337X	NEW YORK /AMERICA
APKHAX	New York/America
B83YXC	New York/America
BEHJY4	New_York/America
BHZGTL	New_York/America
CAKFT3	New York/America
CRPM96	New York/America
DQMCP7	New York/America
ETRARM	New York/America
F3CZRJ	New_York/America

TABLE 1

Question 4 - Settings/Features	
WebCode	**Response**
FCDKRQ	New York/America
FFWFVJ	(UTC-05:00) New_York / (America)
FJHEUY	New York/ America
GBC7GA	New York / America
GDR6K2	New York/America
GNPA6M	New_York/America
GYL92Y	New York/America
HPXMMN	New York/America
HXQXXJ	New York / America
J69MWJ	New_York /America
JYHDML	(UTC-05:00) New_York, (America)
KAXHF3	UTC -5 New York America
KGEDVW	New York/America
MN787Z	New York / USA
N34LXG	New York/America
N6PKXX	America/New_York
N9RLXU	New York/America
NAGYFD	New_York /America
PAWF9K	New York / USA
RUGWR6	New York, America
UR36WT	New_York (America)
VKGQ9D	New York/America
VXNLJ4	New York/America
W94QCK	New York/America
WAU23D	New_York/America
WDTCYD	New York/America
WZ8ZM4	New York/America
X78YBX	America/New_York
XV7BJ2	New York/ America
YMTMH8	America/New_York

TABLE 1

Question 4 - Settings/Features	
WebCode	**Response**
YUUYE6	New York/America
Z6A48L	New York/America
Z8YEXE	New_York/America
ZJRXE7	-05 New York/America

Question 4: What is the set time zone for this device? Provide your answer in the following format: City/Country

Consensus Result: New York/America and all other responses that represent the same time zone.

Expected Response Explanation:

The time zone set on this device can be found in the persist.sys.timezone file. This file can be located at: /Root/property/persist.sys.timezone. The time zone can be verified by looking at the time stamps of various data including Email, Call Log, and Text Messages.

Expected Response Illustration:

Persist.sys.timezone file:

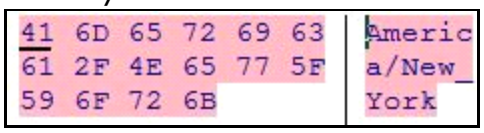


TABLE 1

Question 5 - Settings/Features

Question 5: What is the 15 digit International Mobile Subscriber Identity (IMSI) number associated with the device?

Manufacturer's Expected Response: 311480373589089

WebCode	Response
26L4K9	311480373589089
2HT9U9	311480373589089
3DTGYG	311480373589089
4DUFQ6	311480373589089
4PYWYP	311480373589089
4WN9JF	311480373589089
4ZJ6ZT	311480373589089
64G4UJ	311480373589089
6MTQHC	311480373589089
6XUBJJ	311480373589089
7HDKDP	311480373589089
7Q8P8Q	311480373589089
7XHAQJ	311480373589089
84UA8D	311480373589089
8AWL3B	311480373589089
8Q7ENT	311480373589089
9RWZUN	311480373589089
9WB7YB	311480373589089
AL337X	311480373589089
APKHAX	311480373589089
B83YXC	311480373589089
BEHJY4	311480373589089
BHZGTL	311480373589089
CAKFT3	311480373589089
CRPM96	311480373589089
DQMCP7	311480373589089
ETRARM	311480373589089
F3CZRJ	311480373589089

TABLE 1

Question 5 - Settings/Features	
WebCode	**Response**
FCDKRQ	311480373589089
FFWFVJ	311480373589089
FJHEUY	311480373589089
GBC7GA	311480373589089
GDR6K2	311480373589089
GNPA6M	311480373589089
GYL92Y	311480373589089
HPXMMN	311480373589089
HXQXXJ	311480373589089
J69MWJ	311480373589089
JYHDML	311480373589089
KAXHF3	311480373589085
KGEDVW	311480373589089
MN787Z	311480373589089
N34LXG	311480373589089
N6PKXX	311480373589089
N9RLXU	311480373589089
NAGYFD	311480373589089
PAWF9K	311480373589089
RUGWR6	311480373589089
UR36WT	89148000003668747806
VKGQ9D	311480373589089
VXNLJ4	311480373589089
W94QCK	311480373589089
WAU23D	311480373589089
WDTCYD	311480373589089
WZ8ZM4	311480373589089
X78YBX	311480373589089
XV7BJ2	311480373589089
YMTMH8	311480373589089

TABLE 1

Question 5 - Settings/Features	
WebCode	**Response**
YUUYE6	311480373589089
Z6A48L	311480373589089
Z8YEXE	311480373589089
ZJRXE7	311480373589089

Question 5: What is the 15 digit International Mobile Subscriber Identity (IMSI) number associated with the device?

Consensus Result: 311480373589089

Expected Response Explanation:

The unique 15 digit numeric identifier can be found within a XML file located here: /Root/data/com.google.android.gms/shared_prefs/Checkin.xml

Expected Response Illustration:

XML file:

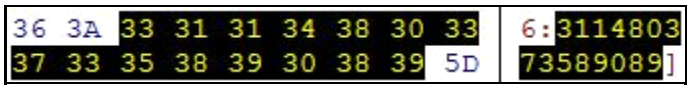


TABLE 1

Question 6 - Settings/Features

Question 6: Provide the MAC address of the device.

Manufacturer's Expected Response: DC:74:A8:DA:F5:0D

WebCode	Response
26L4K9	DC:74:A8:DA:F5:0D
2HT9U9	DC74A8DAF50D
3DTGYG	DC:74:A8:DA:F5:0C
4DUFQ6	DC:74:A8:DA:F5:0D
4PYWYP	Bluetooth: DC:74:A8:DA:F5:0C WiFi: DC:74:A8:DA:F5:0D
4WN9JF	DC:74:A8:DA:F5:0D
4ZJ6ZT	DC:74:A8:DA:F5:0D
64G4UJ	DC:74:A8:DA:F5:0D
6MTQHC	DC:74:A8:DA:F5:0D
6XUBJJ	DC:74:A8:DA:F5:0D
7HDKDP	DC:74:A8:DA:F5:0D
7Q8P8Q	DC:74:A8:DA:F5:0D
7XHAQJ	DC:74:A8:DA:F5:0D
84UA8D	DC:74:A8:DA:F5:0D
8AWL3B	DC:74:A8:DA:F5:0D
8Q7ENT	DC:74:A8:DA:F5:0D
9RWZUN	DC:74:A8:DA:F5:0C
9WB7YB	DC:74:A8:DA:F5:0D
AL337X	DC:74:A8:DA:F5:0D
APKHAX	DC:74:A8:DA:F5:0D
B83YXC	DC:74:A8:DA:F5:0D
BEHJY4	DC:74:A8:DA:F5:0D
BHZGTL	DC:74:A8:DA:F5:0D
CAKFT3	DC:74:A8:DA:F5:0D
CRPM96	DC:74:A8:DA:F5:0D
DQMCP7	DC:74:A8:DA:F5:0D
ETRARM	DC:74:A4:DA:F5:0D
F3CZRJ	DC:74:A8:DA:F5:0D
FCDKRQ	DC:74:A8:DA:F5:0D

TABLE 1

Question 6 - Settings/Features	
WebCode	**Response**
FFWFVJ	DC:74:A8:DA:F5:0C
FJHEUY	DC:74:A8:DA:F5:0D
GBC7GA	DC:74:A8:DA:F5:0D
GDR6K2	DC:74:A8:DA:F5:0D
GNPA6M	DC:74:A8:DA:F5:0D
GYL92Y	DC:74:A8:DA:F5:0D
HPXMMN	DC:74:A8:DA:F5:0D
HXQXXJ	DC:74:A8:DA:F5:0D
J69MWJ	DC:74:A8:DA:F5:0D
JYHDML	DC:74:A8:DA:F5:0D
KAXHF3	DC:74:A8:DA:F5:0D
KGEDVW	DC:74:A8:DA:F5:0C
MN787Z	DC:74:A8:DA:F5:OD
N34LXG	DC:74:A8:DA:F5:0D
N6PKXX	DC:74:A8:DA:F5:0C
N9RLXU	DC:74:A8:DA:F5:0D
NAGYFD	DC:74:A8:DA:F5:0D
PAWF9K	DC:74:A8:DA:F5:0D
RUGWR6	DC:74:A8:DA:F5:0D
UR36WT	DC:74:A8:DA:F5:0D
VKGQ9D	DC:74:A8:DA:F5:0D
VXNLJ4	DC:74:A8:DA:F5:0D
W94QCK	DC:74:A8:DA:F5:0D
WAU23D	DC:74:A8:DA:F5:0D
WDTCYD	DC:74:A8:DA:F5:0D
WZ8ZM4	DC:74:A8:DA:F5:0D
X78YBX	DC:74:A8:DA:F5:0D
XV7BJ2	DC:74:A8:DA:F5:0D
YMTMH8	DC:74:A8:DA:F5:0D, DC:74:A8:DA:F5:0C
YUUYE6	DC:74:A8:DA:F5:0D

TABLE 1

Question 6 - Settings/Features	
WebCode	**Response**
Z6A48L	DC:74:A8:DA:F5:0D
Z8YEXE	DC:74:A8:DA:F5:0D
ZJRXE7	DC:74:A8:DA:F5:0D

Question 6: Provide the MAC address of the device.

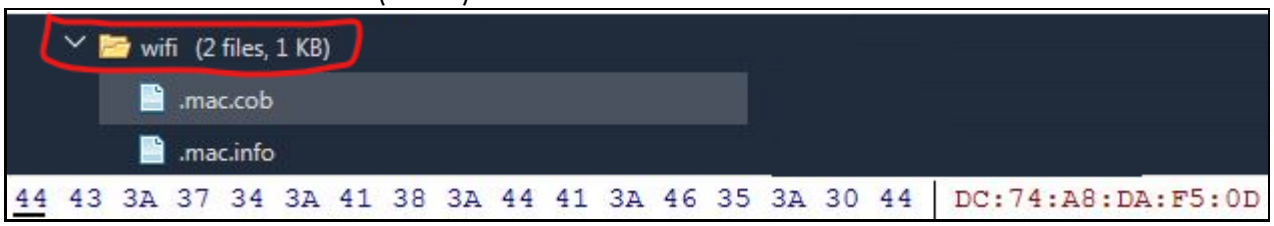
Consensus Result: DC:74:A8:DA:F5:0D or DC:74:A8:DA:F5:0C

Expected Response Explanation:

The expected response was DC:74:A8:DA:F5:0D (MAC address of the wifi radio) however, due to the possible ambiguity of the question, the response DC:74:A8:DA:F5:0C (MAC address of the bluetooth radio) was also accepted. Information regarding the MAC address for the wifi radio and bluetooth radio are found at the following locations, respectively:
/Root/wifi/.mac.info
/Root/bluetooth/bt_addr

Expected Response Illustration:

MAC address of the wifi radio (device):



MAC address of the bluetooth radio:

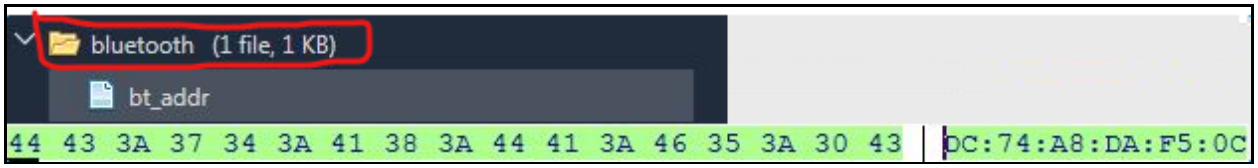


TABLE 1

Question 7 - Settings/Features

Question 7: When was the SIM activated/changed on this device? Provide the answer in UNIX epoch time. Do not round the value. Answer must include milliseconds.

Manufacturer's Expected Response: 1542820248368

WebCode	Response
26L4K9	1542820248368
2HT9U9	1542820248368
3DTGYG	1542820248368 Wednesday, November 21, 2018 12:10:48.368 PM GMT-05:00
4DUFQ6	1542820248368
4PYWYP	1542820248368
4WN9JF	Wed, 21 November 2018 17:10:48.368 (UTC 0) Wed, 21 November 2018 12:10:48:368 (UTC -5)
4ZJ6ZT	1542820248368
64G4UJ	1542820248368
6MTQHC	1542820248368
6XUBJJ	1542820248368
7HDKDP	1542820248368
7Q8P8Q	1542820248368
7XHAQJ	1542820248368
84UA8D	1542820248368
8AWL3B	11/21/2018 12:10:48.368 (UTC-5) 11/21/2018 17:10:48.368 (UTC+0)
8Q7ENT	1542820248368
9RWZUN	1542820248368
9WB7YB	1542820248368
AL337X	21-11-2018 17:10:48 (UTC+0)
APKHAX	1542820248368
B83YXC	1542820248368
BEHJY4	1542820248368
BHZGTL	These are not services we provide as part of our analysis.
CAKFT3	1542820248368
CRPM96	1542820248368
DQMCP7	1542820248000
ETRARM	1542820248368
F3CZRJ	1542820248368

TABLE 1

Question 7 - Settings/Features	
WebCode	**Response**
FCDKRQ	1542820248368
FFWFVJ	1542820248368
FJHEUY	1542820248368
GBC7GA	1542820248368
GDR6K2	1542820248368
GNPA6M	1542820248368
GYL92Y	1542820248368
HPXMMN	1542820248368
HXQXXJ	1542820248368
J69MWJ	11/21/2018 5:10:48 PM(UTC+0)
JYHDML	1451606563000
KAXHF3	1542820248000
KGEDVW	11/21/2018 17:10:48.368 (UTC 0)
MN787Z	1542820248368
N34LXG	1542820248368
N6PKXX	1542820248368
N9RLXU	1542820248368
NAGYFD	1542820248368
PAWF9K	21-Nov-18 5:10:48 PM(UTC+0) SimChangeTime=1542777048
RUGWR6	1542820248.368
UR36WT	1542820248000
VKGQ9D	1542820248368
VXNLJ4	1542820248000
W94QCK	1542820248368
WAU23D	1542820248368
WDTCYD	1542820248368
WZ8ZM4	1542820200000
X78YBX	1542820248368
XV7BJ2	1542820248368
YMTMH8	"1542820222648" or "21-Nov-18 17:10:22"

TABLE 1

Question 7 - Settings/Features	
WebCode	**Response**
YUUYE6	1542820248368
Z6A48L	1542820248368
Z8YEXE	1542820248368
ZJRXE7	1542820248000

Question 7: When was the SIM activated/changed on this device? Provide the answer in UNIX epoch time. Do not round the value. Answer must include milliseconds.

Consensus Result: 1542820248368 and all formatting styles which represent the same date and time. Although the question requested the time to include milliseconds, participants that reported the consensus date and time excluding the milliseconds were also accepted.

Expected Response Explanation:

Information regarding when the SIM was activated/changed is located here:
/Root/system/SimCard.dat

Expected Response Illustration:

SIM activated/changed time:

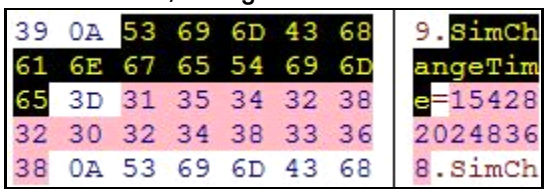


TABLE 1

Question 8 - Settings/Features

Question 8: Provide the operating system (OS) version installed on the device.

Manufacturer's Expected Response: 6.0.1

WebCode	Response
26L4K9	6.0.1
2HT9U9	6.0.1
3DTGYG	6.0.1
4DUFQ6	6.0.1
4PYWYP	6.0.1
4WN9JF	6.0.1
4ZJ6ZT	6.0.1
64G4UJ	6.0.1
6MTQHC	Android 6.0.1
6XUBJJ	6.0.1
7HDKDP	6.0.1
7Q8P8Q	6.0.1
7XHAQJ	Android version 6.0.1
84UA8D	6.0.1
8AWL3B	6.0.1
8Q7ENT	6.0.1
9RWZUN	6.0.1
9WB7YB	Android 6.0.1
AL337X	Android 6.0.1
APKHAX	6.0.1
B83YXC	6.0.1
BEHJY4	6.0.1
BHZGTL	6.0.1
CAKFT3	6.0.1
CRPM96	6.0.1
DQMCP7	6.0.1
ETRARM	6.0.1
F3CZRJ	6.0.1
FCDKRQ	Android 6.0.1

TABLE 1

Question 8 - Settings/Features	
WebCode	**Response**
FFWFVJ	6.0.1
FJHEUY	6.0.1
GBC7GA	Android 6.0.1
GDR6K2	6.0.1
GNPA6M	6.0.1
GYL92Y	6.0.1
HPXMMN	6.0.1
HXQXXJ	6.0.1
J69MWJ	6.0.1
JYHDML	6.0.1
KAXHF3	Android 6.0.1
KGEDVW	6.0.1
MN787Z	6.0.1
N34LXG	6.0.1
N6PKXX	6.0.1
N9RLXU	6.0.1
NAGYFD	6.0.1
PAWF9K	6.0.1
RUGWR6	6.0.1
UR36WT	6.0.1
VKGQ9D	6.0.1
VXNLJ4	6.0.1
W94QCK	6.0.1
WAU23D	6.0.1
WDTCYD	Android 6.0.1
WZ8ZM4	6.0.1
X78YBX	6.0.1
XV7BJ2	6.0.1
YMTMH8	6.0.1
YUUYE6	6.0.1

TABLE 1

Question 8 - Settings/Features	
WebCode	**Response**
Z6A48L	6.0.1
Z8YEXE	6.0.1
ZJRXE7	Android 6.0.1

Question 8: Provide the operating system (OS) version installed on the device.

Consensus Result: 6.0.1

Expected Response Explanation:

Information regarding the version of the operating system version installed on this device is located here: /Root/build.prop

Expected Response Illustration:

OS version installed on the device:

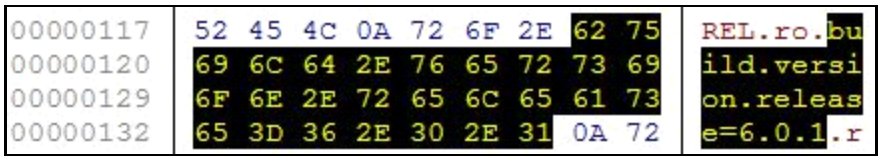


TABLE 1

Question 9 - Settings/Features

Question 9: As per the Bluetooth configuration file, this device was connected to a vehicle. Provide the bluetooth name to which this device was connected to last.

Manufacturer's Expected Response: HandsFreeLink

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
26L4K9	HandsFreeLink
2HT9U9	HandsFreeLink
3DTGYG	HandsFreeLink
4DUFQ6	HandsFreeLink
4PYWYP	HandsFreeLink
4WN9JF	Galaxy J7 Sky Pro
4ZJ6ZT	Motorola IHF1000
64G4UJ	HandsFreeLink
6MTQHC	
6XUBJJ	HandsFreeLink
7HDKDP	Motorola IHF1000
7Q8P8Q	Motorola IHF1000
7XHAQJ	Motorola IHF1000
84UA8D	
8AWL3B	Galaxy J7 Sky Pro
8Q7ENT	HandsFreeLink
9RWZUN	HandsFreeLink
9WB7YB	HandsFreeLink
AL337X	34:C7:31 = Honda Pilot 2016 handsfreelink..
APKHAX	Not found
B83YXC	Galaxy J7 Sky Pro
BEHJY4	HandsFreeLink
BHZGTL	Honda Pilot 2016 handsfreelink
CAKFT3	HandsFreeLink
CRPM96	HandsFreeLink
DQMCP7	Audi MMI
ETRARM	HandsFreeLink
F3CZRJ	

TABLE 1

Question 9 - Settings/Features		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
FCDKRQ	HandsFreeLink	
FFWFVJ	Honda Pilot 2016 handsfreelink..	
FJHEUY	Galaxy J7 Sky Pro	
GBC7GA	Honda Pilot 2016 handsfreelink	
GDR6K2	HandsFreeLink	
GNPA6M	HeadsetStateMachine	
GYL92Y	HandsFreeLink	
HPXMMN	HandsFreeLink	
HXQXXJ		
J69MWJ		
JYHDML	auto_pair_devlist.conf	
KAXHF3	No Bluetooth connections are located within the data.	
KGEDVW	HandsFreeLink	
MN787Z	device not showing any connection to a vehicles bluetooth	
N34LXG	HandsFreeLink	
N6PKXX	Unable to answer	
N9RLXU	HandsFreeLink	
NAGYFD	HandsFreeLink	
PAWF9K	HandsFreeLink	
RUGWR6	HandsFreeLink	
UR36WT	no such file or contents	
VKGQ9D	HandsFreeLink	
VXNLJ4		
W94QCK	HandsFreeLink	
WAU23D	HandsFreeLink	
WDTCYD	HandsFreeLink	
WZ8ZM4	0c:d9:c1:2f:c1:9c	
X78YBX	11/28/2018 12:16:48 PM Motorola IHF1000, BMW/Audi car	
XV7BJ2	Motorola IHF1000	
YMTMH8	vzims.com	

TABLE 1

Question 9 - Settings/Features		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
YUUYE6	HandsFreeLink	
Z6A48L	Galaxy J7 Sky Pro	
Z8YEXE	HandsFreeLink	
ZJRXE7	HandsFreeLink	

Question 9: As per the Bluetooth configuration file, this device was connected to a vehicle. Provide the bluetooth name to which this device was connected to last.

Consensus Result: A consensus was not achieved. The objective of this question was to locate the Bluetooth configuration file and identify the name listed in this file for the bluetooth device.

Expected Response Explanation:

The expected response was Hands Free Link. A non-consensus majority of participants reported the expected response, however other participants reported either the model of the phone or the model of the bluetooth device and 11 participants did not report a response or mentioned that the name was not found.
Information regarding the name of the Bluetooth last connected to this device is located here:
userdata (ExtX)/Root/misc/bluedroid/bt_config.conf

Expected Response Illustration:

Bluetooth Name:

TABLE 1

Question 10 - Settings/Features

Question 10: Provide the date and time of when this device was last turned on. Answer using the time zone set on the device using the following format: Month/Date/Year Hour:Minutes AM/PM

Manufacturer's Expected Response: 12/3/2018 08:19 AM

WebCode	Response
26L4K9	12/3/2018 8:19 AM
2HT9U9	12/03/2018 8:19 AM
3DTGYG	12/03/2018 08:19 AM
4DUFQ6	12/3/2018 08:19 AM
4PYWYP	12/03/2018 08:19 AM
4WN9JF	12/3/2018 08:19 AM (UTC -5)
4ZJ6ZT	12/03/2018 8:19:52 AM
64G4UJ	12/03/2018 8:19 AM
6MTQHC	12/3/2018 08:19 AM
6XUBJJ	12/3/2018 8:19:52 AM
7HDKDP	12/3/2018 8:19:52 AM
7Q8P8Q	12/03/2018 08:19:52AM
7XHAQJ	12/03/2018 08:19 AM
84UA8D	12/3/2018 8:19 AM
8AWL3B	12/3/2018 8:19:52 AM (UTC-5)
8Q7ENT	12/03/2018 08:19:52 AM (UTC-5)
9RWZUN	12/3/2018 08:19 AM
9WB7YB	12/3/2018 8:19 AM
AL337X	3/12/2018 08:19:28 (UTC-5)
APKHAX	12/03/2018 08:19 AM
B83YXC	11/27/2018 08:35 AM
BEHJY4	12/3/2018 1:19 PM
BHZGTL	12/3/2018 08:19 AM
CAKFT3	12/3/2018 8:19 AM
CRPM96	12/3/2018 08:19 AM
DQMCP7	12/3/2018 8:19:52 AM
ETRARM	12/3/18 8:19 AM
F3CZRJ	12/3/2018 8:19 AM

TABLE 1

Question 10 - Settings/Features	
WebCode	**Response**
FCDKRQ	12/3/2018 08:19 AM
FFWFVJ	12/3/2018 08:19 (UTC-5)
FJHEUY	12/2/2018 8:19 AM
GBC7GA	12/03/2018 08:19 AM
GDR6K2	12/03/2018 08:19 AM
GNPA6M	12/03/2108 08:19 AM
GYL92Y	12/3/2018 8:19 AM
HPXMMN	12/03/2018 8:19 AM
HXQXXJ	12/3/2018 08:19 AM
J69MWJ	12/3/2018 8:19:52 AM (UTC-5)
JYHDML	12/3/2018 8:19 AM
KAXHF3	12/3/2018 8:19 AM
KGEDVW	12/03/2018 8:19 AM (UTC-5)
MN787Z	12/3/2018 8:19:52 AM (UTC-5)
N34LXG	12/03/2018 08:59 AM
N6PKXX	12/3/2018 8:19:52 AM
N9RLXU	12/3/2018 8:19 AM
NAGYFD	12/03/2018 08:19 AM
PAWF9K	Dec/03/18 8:19 AM
RUGWR6	12/3/2018 8:19 AM
UR36WT	12/3/2018 8:19 AM
VKGQ9D	12/03/2018 08:19 AM
VXNLJ4	12/03/2018 8:19 AM
W94QCK	12/3/2018 8:19:52 AM
WAU23D	12/03/2018 8:19 AM
WDTCYD	12/03/2018 08:19:52 AM
WZ8ZM4	12/3/2018 08:19 (UTC-5)
X78YBX	12/3/2018 08:16:29 AM
XV7BJ2	12/03/18 08:19 AM
YMTMH8	Date: Dec/18/2018, Time: 11.00 AM (UTC_Time is 3:00 PM Convert from UTC-4 hours.)

TABLE 1

Question 10 - Settings/Features	
WebCode	**Response**
YUUYE6	12/3/2018 8:19 AM
Z6A48L	12/3/2018 8:19:52 AM
Z8YEXE	12/03/2018 08:19 AM
ZJRXE7	12/3/2018 08:19:52 AM

Question 10: Provide the date and time of when this device was last turned on. Answer using the time zone set on the device using the following format: Month/Date/Year Hour:Minutes AM/PM

Consensus Result: 12/3/2018 08:19 AM

Expected Response Explanation:

The source for this information can be found within the blk0_mmcvlk0.bin at offset: 0x224E9A000

Expected Response Illustration:

Powering event information:

#		Timestamp	Event
1		12/3/2018 08:19 AM(UTC-5)	On
2		12/3/2018 08:16 AM(UTC-5)	On
3		11/30/2018 08:59 AM(UTC-5)	On
4	✖	11/29/2018 08:29 AM(UTC-5)	On
5	✖	11/28/2018 03:29 PM(UTC-5)	On

TABLE 1

Question 11 - Settings/Features

Question 11: How many wireless networks was this device connected to?

Manufacturer's Expected Response: Three (3)

WebCode	Response
26L4K9	3
2HT9U9	3
3DTGYG	Three (3)
4DUFQ6	3
4PYWYP	3
4WN9JF	3
4ZJ6ZT	3
64G4UJ	3
6MTQHC	3
6XUBJJ	3
7HDKDP	3
7Q8P8Q	3
7XHAQJ	3
84UA8D	3
8AWL3B	3
8Q7ENT	3
9RWZUN	Three
9WB7YB	3
AL337X	3
APKHAX	3
B83YXC	3
BEHJY4	Three(3)
BHZGTL	3
CAKFT3	3
CRPM96	3
DQMCP7	3
ETRARM	3
F3CZRJ	3
FCDKRQ	Three

TABLE 1

Question 11 - Settings/Features	
WebCode	**Response**
FFWFVJ	1 TGI Fridays Guest Wifi
FJHEUY	3
GBC7GA	3
GDR6K2	3
GNPA6M	3
GYL92Y	3
HPXMMN	3
HXQXXJ	3
J69MWJ	3
JYHDML	3
KAXHF3	3
KGEDVW	3
MN787Z	3
N34LXG	3
N6PKXX	3
N9RLXU	3
NAGYFD	3
PAWF9K	3
RUGWR6	3
UR36WT	3
VKGQ9D	3
VXNLJ4	3
W94QCK	3
WAU23D	3
WDTCYD	3
WZ8ZM4	3
X78YBX	3
XV7BJ2	3
YMTMH8	3
YUUYE6	3

TABLE 1

Question 11 - Settings/Features	
WebCode	**Response**
Z6A48L	3
Z8YEXE	3
ZJRXE7	3

Question 11: How many wireless networks was this device connected to?

Consensus Result: Three (3)

Expected Response Explanation:

Information regarding wireless networks connected to this device is located here:
/Root/misc/wifi/wpa_supplicant.conf

Expected Response Illustration:

Wireless connections:

#	SSId
1	TGI Fridays Guest Wifi
2	BobEvansPublic
3	PANERA

TABLE 1

Question 12 - Settings/Features

Question 12: What is the most used 5 digit Location Area Code (LAC) by this device?

Manufacturer's Expected Response: 29953

WebCode	Response
26L4K9	29553
2HT9U9	29953
3DTGYG	29953
4DUFQ6	29953
4PYWYP	29953
4WN9JF	29953
4ZJ6ZT	29953
64G4UJ	29953
6MTQHC	29953
6XUBJJ	29953
7HDKDP	29953
7Q8P8Q	29953
7XHAQJ	29953
84UA8D	29953
8AWL3B	29953
8Q7ENT	29953
9RWZUN	29953
9WB7YB	29953
AL337X	29953
APKHAX	29953
B83YXC	29953
BEHJY4	29953
BHZGTL	These are not services we provide as part of our analysis.
CAKFT3	29953
CRPM96	29953
DQMCP7	20176
ETRARM	29953
F3CZRJ	29953
FCDKRQ	29953

TABLE 1

Question 12 - Settings/Features	
WebCode	**Response**
FFWFVJ	29953
FJHEUY	29953
GBC7GA	29953
GDR6K2	29953
GNPA6M	29953
GYL92Y	29953
HPXMMN	70354
HXQXXJ	29953
J69MWJ	29953
JYHDML	29953
KAXHF3	29953
KGEDVW	29953
MN787Z	29953
N34LXG	29953
N6PKXX	39953
N9RLXU	29953
NAGYFD	29953
PAWF9K	LAC : 29953
RUGWR6	29953
UR36WT	29953
VKGQ9D	703
VXNLJ4	29953
W94QCK	29953
WAU23D	29953
WDTCYD	29953
WZ8ZM4	31148
X78YBX	29953
XV7BJ2	29953
YMTMH8	51830
YUUYE6	29953

TABLE 1

Question 12 - Settings/Features	
WebCode	**Response**
Z6A48L	29953
Z8YEXE	29953
ZJRXE7	29953 29953

Question 12: What is the most used 5 digit Location Area Code (LAC) by this device?

Consensus Result: 29953

Expected Response Explanation:

Information regarding Location Area Codes used by this device is located here:
userdata (ExtX)/Root/data/com.google.android.gms/databases/herrevad
Table: local_reports

Expected Response Illustration:

LAC used by device:

TimeStamp	LAC	CID	Type	Package
11/27/2018 08:34 AM(UTC-5)	29953	29974531	GSM	Play Store
11/27/2018 08:33 AM(UTC-5)	29953	29974531	GSM	Play Store
11/27/2018 08:31 AM(UTC-5)	29953	29974531	GSM	Gmail
11/27/2018 08:25 AM(UTC-5)	29953	29974531	GSM	Maps

TABLE 1

Question 13 - Email

Question 13: What is the Google e-mail account associated with this device?

Manufacturer's Expected Response: diazcarlos1185@gmail.com

WebCode	Response
26L4K9	diazcarlos1185@gmail.com
2HT9U9	diazcarlos1185@gmail.com
3DTGYG	diazcarlos1185@gmail.com
4DUFQ6	diazcarlos1185@gmail.com
4PYWYP	diazcarlos1185@gmail.com
4WN9JF	diazcarlos1185@gmail.com
4ZJ6ZT	diazcarlos1185@gmail.com
64G4UJ	diazcarlos1185@gmail.com
6MTQHC	diazcarlos1185@gmail.com
6XUBJJ	diazcarlos1185@gmail.com
7HDKDP	diazcarlos1185@gmail.com
7Q8P8Q	diazcarlos1185@gmail.com
7XHAQJ	diazcarlos1185@gmail.com
84UA8D	diazcarlos1185@gmail.com
8AWL3B	diazcarlos1185@gmail.com
8Q7ENT	diazcarlos1185@gmail.com
9RWZUN	diazcarlos1185@gmail.com
9WB7YB	diazcarlos1185@gmail.com
AL337X	diazcarlos1185@gmail.com
APKHAX	diazcarlos1185@gmail.com
B83YXC	diazcarlos1185@gmail.com
BEHJY4	diazcarlos1185@gmail.com
BHZGTL	diazcarlos1185@gmail.com
CAKFT3	diazcarlos1185@gmail.com
CRPM96	diazcarlos1185@gmail.com
DQMCP7	diazcarlos1185@gmail.com
ETRARM	diazcarlos1185@gmail.com
F3CZRJ	diazcarlos1185@gmail.com
FCDKRQ	diazcarlos1185@gmail.com

TABLE 1

Question 13 - Email	
WebCode	**Response**
FFWFVJ	diazcarlos1185@gmail.com
FJHEUY	diazcarlos1185@gmail.com
GBC7GA	diazcarlos1185@gmail.com
GDR6K2	diazcarlos1185@gmail.com
GNPA6M	diazcarlos1185@gmail.com
GYL92Y	diazcarlos1185@gmail.com
HPXMMN	diazcarlos1185@gmail.com
HXQXXJ	diazcarlos1185@gmail.com
J69MWJ	diazcarlos1185@gmail.com
JYHDML	diazcarlos1185@gmail.com
KAXHF3	diazcarlos1185@gmail.com
KGEDVW	diazcarlos1185@gmail.com
MN787Z	diazcarlos1185@gmail.com
N34LXG	diazcarlos1185@gmail.com
N6PKXX	diazcarlos1185@gmail.com
N9RLXU	diazcarlos1185@gmail.com
NAGYFD	diazcarlos1185@gmail.com
PAWF9K	diazcarlos1185@gmail.com
RUGWR6	diazcarlos1185@gmail.com
UR36WT	diazcarlos1185@gmail.com
VKGQ9D	diazcarlos1185@gmail.com
VXNLJ4	diazcarlos1185@Gmail.com
W94QCK	diazcarlos1185@gmail.com
WAU23D	diazcarlos1185@gmail.com
WDTCYD	diazcarlos1185@gmail.com
WZ8ZM4	diazcarlos1185@gmail.com
X78YBX	diazcarlos1185@gmail.com
XV7BJ2	diazcarlos1185@gmail.com
YMTMH8	diazcarlos1185@gmail.com
YUUYE6	diazcarlos1185@gmail.com

TABLE 1

Question 13 - Email	
WebCode	**Response**
Z6A48L	diazcarlos1185@gmail.com
Z8YEXE	diazcarlos1185@gmail.com
ZJRXE7	"Carlos Diaz" diazcarlos1185@gmail.com

Question 13: What is the Google e-mail account associated with this device?

Consensus Result: diazcarlos1185@gmail.com

Expected Response Explanation:

The Google e-mail account associated with this device is "diazcarlos1185@gmail.com". The account information can be found within the accounts database which can be located at:
/Root/system/users/0/accounts.db

Expected Response Illustration:

Email Account information:

Name	Username	Service Type
	diazcarlos1185@gmail.com	com.google
Carlos Diaz	diazcarlos1185@gmail.com	Google Photos
Carlos Diaz	diazcarlos1185@gmail.com	Google Drive
diazcarlos1185@gmail.com	1543328568390	Google Client ID

TABLE 1

Question 14 - Email

Question 14: In a travel inquiry email sent to "travel@travelharmony.com" on 11/28/2018 at 10:28 AM(UTC-5), what was the requested destination? Provide the name of the destination only, not the complete email.

Manufacturer's Expected Response: Bermuda

WebCode	Response
26L4K9	Bermuda
2HT9U9	Bermuda
3DTGYG	Bermuda
4DUFQ6	Bermuda
4PYWYP	Bermuda
4WN9JF	Bermuda
4ZJ6ZT	Bermuda
64G4UJ	Bermuda
6MTQHC	Bermuda
6XUBJJ	Bermuda
7HDKDP	Bermuda
7Q8P8Q	Bermuda
7XHAQJ	Bermuda
84UA8D	Bermuda
8AWL3B	Bermuda
8Q7ENT	Bermuda
9RWZUN	Bermuda
9WB7YB	Bermuda
AL337X	Bermudas
APKHAX	Bermuda
B83YXC	Bermuda
BEHJY4	Bermuda
BHZGTL	Bermuda
CAKFT3	Bermuda
CRPM96	Bermuda
DQMCP7	Bermuda
ETRARM	Bermuda

TABLE 1

Question 14 - Email	
WebCode	**Response**
F3CZRJ	Bermuda
FCDKRQ	Bermuda
FFWFVJ	Bermuda
FJHEUY	Bermuda
GBC7GA	Bermuda
GDR6K2	Bermuda
GNPA6M	Bermuda
GYL92Y	Bermuda
HPXMMN	Bermuda
HXQXXJ	Bermuda
J69MWJ	Bermuda
JYHDML	Bermuda
KAXHF3	Bermuda
KGEDVW	Bermuda
MN787Z	Bermuda
N34LXG	Bermuda
N6PKXX	Bermuda
N9RLXU	Bermuda
NAGYFD	Bermuda
PAWF9K	Bermuda
RUGWR6	Bermuda
UR36WT	Bermuda
VKGQ9D	Bermuda
VXNLJ4	Bermuda
W94QCK	Bermuda
WAU23D	Bermuda
WDTCYD	Bermuda
WZ8ZM4	Bermuda
X78YBX	Bermuda
XV7BJ2	Bermuda

TABLE 1

Question 14 - Email	
WebCode	**Response**
YMTMH8	Bermuda
YUUYE6	Bermuda
Z6A48L	Bermuda
Z8YEXE	Bermuda
ZJRXE7	Bermuda

Question 14: In a travel inquiry email sent to "travel@travelharmony.com" on 11/28/2018 at 10:28 AM(UTC-5), what was the requested destination? Provide the name of the destination only, not the complete email.

Consensus Result: Bermuda

Expected Response Explanation:

Information regarding the text found within the e-mail sent to the specified email address is located here: /Root/data/com.google.android.gm/databases/mailstore.diazcarlos1185@gmail.com.db

Expected Response Illustration:

Email information:

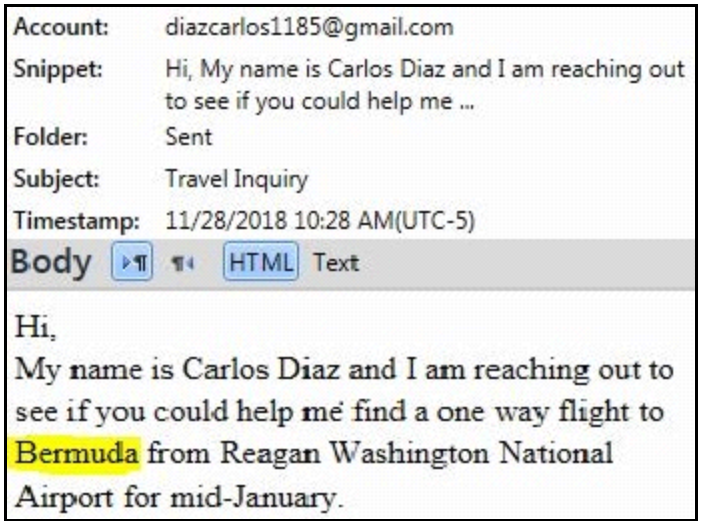


TABLE 1

Question 15 - Email

Question 15: Provide the subject of the email associated with Message ID "16184799431074416 24" and Conversation ID "16184799098367675 20".

Manufacturer's Expected Response: Meeting Location

WebCode	Response
26L4K9	Meeting Location
2HT9U9	Meeting Location
3DTGYG	Meeting Location
4DUFQ6	Meeting Location
4PYWYP	Meeting Location
4WN9JF	Meeting Location
4ZJ6ZT	Meeting Location
64G4UJ	Meeting Location
6MTQHC	Meeting location
6XUBJJ	Meeting Location
7HDKDP	Meeting Location
7Q8P8Q	Meeting Location
7XHAQJ	Meeting Location
84UA8D	Meeting Location
8AWL3B	Meeting Location
8Q7ENT	Meeting Location
9RWZUN	Meeting Location
9WB7YB	Meeting Location
AL337X	Meeting Location
APKHAX	Meeting Location
B83YXC	Meeting Location
BEHJY4	Meeting Location
BHZGTL	Meeting Location
CAKFT3	Meeting Location
CRPM96	Meeting location
DQMCP7	Meeting Location
ETRARM	Meeting Location
F3CZRJ	Meeting Location

TABLE 1

Question 15 - Email	
WebCode	**Response**
FCDKRQ	Meeting Location
FFWFVJ	Meeting Location
FJHEUY	Meeting Location
GBC7GA	Meeting Location
GDR6K2	Meeting Location
GNPA6M	Meeting Location
GYL92Y	Meeting Location
HPXMMN	Meeting Location
HXQXXJ	Meeting Location
J69MWJ	Meeting Location
JYHDML	Meeting Location
KAXHF3	Meeting Location
KGEDVW	Meeting Location
MN787Z	Meeting Location
N34LXG	Meeting Location
N6PKXX	Meeting Location
N9RLXU	Meeting Location
NAGYFD	Meeting Location
PAWF9K	Meeting Location
RUGWR6	Meeting Location
UR36WT	Meeting Location
VKGQ9D	Meeting Location
VXNLJ4	Meeting Location
W94QCK	Meeting Location
WAU23D	Meeting Location
WDTCYD	Meeting Location
WZ8ZM4	Meeting Location
X78YBX	Meeting Location
XV7BJ2	Re: Meeting Location
YMTMH8	Meeting Location

TABLE 1

Question 15 - Email	
WebCode	**Response**
YUUYE6	Meeting Location
Z6A48L	Meeting Location
Z8YEXE	Meeting Location
ZJRXE7	Meeting Location

Question 15: Provide the subject of the email associated with Message ID "16184799431074416 24" and Conversation ID "1618479909836767520".

Consensus Result: Meeting Location

Expected Response Explanation:

Information regarding sent and received emails can be found in the messages table within mailstore.diazcarlos1185@gmail.com. This file is located at: /Root/data/com.google.android.gm/databases/mailstore.diazcarlos1185@gmail.com.db

Expected Response Illustration:

Email information:

messageId	conversation	fromAddress	toAddresses	subject
1618479943107441624	1618479909836767520	"Carlos Diaz" <diazcarlos1185@gmail.com>	"" <dani.polanco90@yahoo.com>	Meeting Location

TABLE 1

Question 16 - Email

Question 16: Provide the names of all the drugs listed in the email received on 1543511979025. Separate the answer using a comma (,)

Manufacturer's Expected Response: Marijuana, Heroin, cocaine

WebCode	Response
26L4K9	Marijuana, Heroin, and cocaine
2HT9U9	Marijuana, Heroin, Cocaine
3DTGYG	Marijuana, Heroin, Cocaine.
4DUFQ6	Marijuana, Heroin, cocaine
4PYWYP	Marijuana, heroin, cocaine
4WN9JF	Marijuana, Heroin, Cocaine (There was a picture of a new product labeled "K2-Spice" contained in the email as well)
4ZJ6ZT	Marijuana, Heroin, and cocaine
64G4UJ	Marijuana,Heroin,Cocaine
6MTQHC	Marijuana, Heroin, cocaine
6XUBJJ	Marijuana, Heroin, cocaine
7HDKDP	Marijuana, Heroin, cocaine
7Q8P8Q	Marijuana, Heroin, Cocaine
7XHAQJ	Marijuana,Heroin,cocaine
84UA8D	Marijuana, Heroin, cocaine
8AWL3B	Marijuana, Heroin, and cocaine (not listed, but K2-spice was the name of a photo)
8Q7ENT	Marijuana, Heroin, cocaine
9RWZUN	Marijuana, Heroin, cocaine
9WB7YB	Marijuana, Heroin, cocaine
AL337X	marijuana, heroin, cocaine
APKHAX	Marijuana, Heroin, cocaine.
B83YXC	Marijuana, Heroin, cocaine
BEHJY4	Marijuana,Heroin,Cocaine
BHZGTL	Marijuana, Heroin, Cocaine, K2-Spice
CAKFT3	Marijuana, Heroin, cocaine
CRPM96	Marijuana, Heroin, cocaine
DQMCP7	Marijuana, Heroin, Cocaine
ETRARM	Marijuana, Heroin, Cocaine
F3CZRJ	Marijuana, Heroin, cocaine

TABLE 1

Question 16 - Email	
WebCode	**Response**
FCDKRQ	Marijuana, Heroin, cocaine
FFWFVJ	Marijuana, Heroin, cocaine
FJHEUY	Marijuana, Heroin, cocaine
GBC7GA	Marijuana, Heroin, and cocaine
GDR6K2	Marijuana, Heroin, cocaine, K2-Spice
GNPA6M	Marijuana,Heroin,cocaine
GYL92Y	Marijuana, Heroin, cocaine
HPXMMN	Marijuana, Heroin, cocaine
HXQXXJ	Marijuana, Heroin, cocaine
J69MWJ	Marijuana, Heroin,and cocaine
JYHDML	Marijuana, Heroin, and cocaine
KAXHF3	Marijuana, Heroin, Cocaine, K2
KGEDVW	Marijuana, Heroin, cocaine
MN787Z	Marijuana, Heroin,cocaine
N34LXG	Marijuana, Heroin, Cocaine.
N6PKXX	Marijuana, Heroin, and cocaine
N9RLXU	Marijuana, Heroin, cocaine
NAGYFD	Marijuana, Heroin, cocaine
PAWF9K	Marijuana, Heroin, and cocaine
RUGWR6	Marijuana, Heroin, Cocaine
UR36WT	Marijuana, Heroin, cocaine
VKGQ9D	Marijuana, Heroin, Cocaine
VXNLJ4	Marijuana, Heroin, Cocaine
W94QCK	Marijuana,Heroin,cocaine
WAU23D	Marijuana, Heroin, cocaine
WDTCYD	Marijuana, Heroin, Cocaine
WZ8ZM4	Marijuana, heroin, cocaine
X78YBX	K2-Spice
XV7BJ2	Marijuana, Heroin, and cocaine
YMTMH8	K2, Spice

TABLE 1

Question 16 - Email	
WebCode	**Response**
YUUYE6	Marijuana, Heroin, cocaine
Z6A48L	Marijuana, Heroin, cocaine
Z8YEXE	Marijuana, Heroin, cocaine
ZJRXE7	Marijuana, Heroin, cocaine

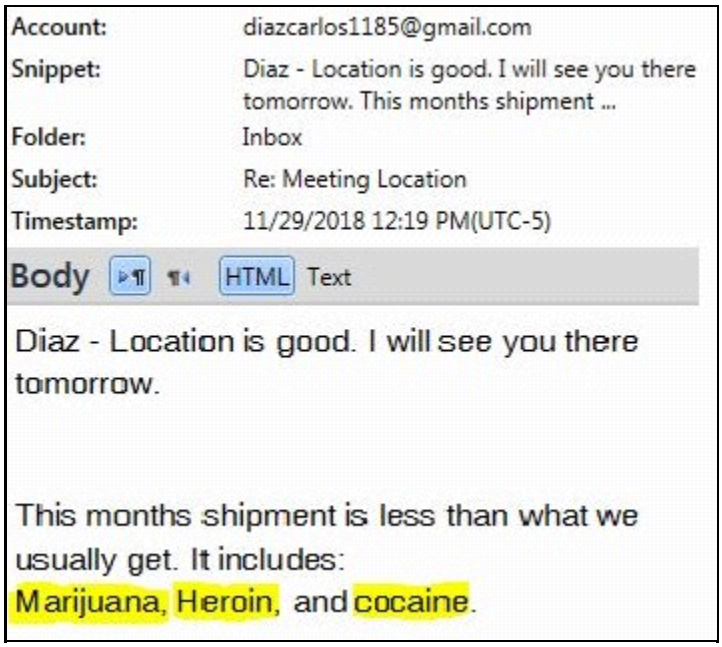
Question 16: Provide the names of all the drugs listed in the email received on 1543511979025. Separate the answer using a comma (,)

Consensus Result: Marijuana, Heroin, cocaine including or excluding K2-spice

Expected Response Explanation:
Information regarding the text found within a received email is located here:
/Root/data/com.google.android.gm/databases/mailstore.diazcarlos1185@gmail.com.db

Expected Response Illustration:

Email information:



Other Responses:
Five participants reported the expected three drugs as well as K2-spice which was the name of the photo attached to the e-mail. The inclusion of K2-spice in the response along with the other three drugs was also accepted.

TABLE 1

Question 17 - Email

Question 17: Provide the epoch timestamp of the last email sent to John Fuller at "Johnfuller82@yahoo.com". Do not round the value. Answer must include milliseconds.

Manufacturer's Expected Response: 1543513804000

WebCode	Response
26L4K9	1543515928000
2HT9U9	1543513804000
3DTGYG	1543495800000
4DUFQ6	1543513804000
4PYWYP	1543513804000
4WN9JF	Thurs, 29 November 2018 17:50:04.000 (UTC 0) Thurs, 29 November 2018 12:50:04.000 (UTC -5)
4ZJ6ZT	1543513804000
64G4UJ	154351380400
6MTQHC	1543513800000
6XUBJJ	1543513804259
7HDKDP	1543513804000
7Q8P8Q	1543513804000
7XHAQJ	1543513804000
84UA8D	1543513804000
8AWL3B	11/29/2018 12:50:04.000 PM (UTC-5) 1543513804000
8Q7ENT	1543513804000
9RWZUN	1543513800
9WB7YB	1543513804000
AL337X	1543513804259
APKHAX	1543513804000
B83YXC	1543513804259
BEHJY4	1543513804000
BHZGTL	These are not services we provide as part of our analysis.
CAKFT3	1543513804259
CRPM96	1543513804000
DQMCP7	1543513804000
ETRARM	1543513804000
F3CZRJ	1543513804000

TABLE 1

Question 17 - Email	
WebCode	**Response**
FCDKRQ	1543513804000
FFWFVJ	1543513804259
FJHEUY	1543445879000
GBC7GA	1543513804000
GDR6K2	1543513804000
GNPA6M	1543513804259
GYL92Y	1543513804000
HPXMMN	1543495804000
HXQXXJ	1543513804000
J69MWJ	12:50:04 PM(UTC-5)
JYHDML	1543495804000
KAXHF3	1543513804000
KGEDVW	Thu, 29 November 2018 17:50:04.000 (UTC 0)
MN787Z	1543513804000
N34LXG	1543495804000
N6PKXX	1543513804000
N9RLXU	1543513804000
NAGYFD	1543513804000
PAWF9K	29-Nov-18 05:50:04 PM 1543488604
RUGWR6	1543513804.000
UR36WT	1542909004000
VKGQ9D	1543513804000
VXNLJ4	1543513804000
W94QCK	1543513804000
WAU23D	1543513804000
WDTCYD	1543513804000
WZ8ZM4	1543513804000
X78YBX	1543515928000
XV7BJ2	1543513800000
YMTMH8	"1543513804000" or "1543513804259" = "29-Nov-18 17:50:04"

TABLE 1

Question 17 - Email	
WebCode	**Response**
YUUYE6	1543513804000
Z6A48L	1543513804000
Z8YEXE	1543513804000
ZJRXE7	1543510204000

Question 17: Provide the epoch timestamp of the last email sent to John Fuller at "Johnfuller82@yahoo.com". Do not round the value. Answer must include milliseconds.

Consensus Result: 1543513804000 and all formatting styles which represent the same date and time. Although the question requested the time to include milliseconds, participants that reported the consensus date and time excluding the milliseconds were also accepted. With milliseconds excluded, participants that reported the "received" timestamp of the last email to John Fuller (instead of "sent" timestamp) were accepted.

Expected Response Explanation:

Information regarding sent and received emails can be found in the messages table within mailstore.diazcarlos1185@gmail.com. This file is located at: /Root/data/com.google.android.gm/databases/mailstore.diazcarlos1185@gmail.com.db-wal

Expected Response Illustration:

Email information:

fromAddress	toAddresses	replyToAddresses	dateSentMs	dateReceivedMs
"Dani Polanco" <dani.polanco90@yahoo.com>	"Carlos Diaz" <diazcarlos1185@gmail.com>		1543511975000	1543511979025
"Carlos Diaz" <diazcarlos1185@gmail.com>	"John Fuller" <Johnfuller82@yahoo.com>		1543513804000	1543513804259
"Google Play" <welcome-googleplay-noreply@google.com>	"" <diazcarlos1185@gmail.com>	"Google Play" <welcome-googleplay-noreply@google.com>	1543513966000	1543513966550
"John Fuller" <johnfuller82@yahoo.com>	"Carlos Diaz" <diazcarlos1185@gmail.com>		1543515928000	1543515932296

TABLE 1

Question 18 - Internet History

Question 18: What was the last term searched using the Mozilla Firefox search engine?

Manufacturer's Expected Response: grams to ounce conversion

WebCode	Response
26L4K9	grams to ounce conversion
2HT9U9	grams to ounce conversion
3DTGYG	grams to ounce conversion
4DUFQ6	grams to ounce conversion
4PYWYP	grams to ounce conversion
4WN9JF	grams to ounce conversion
4ZJ6ZT	grams to ounce conversion
64G4UJ	Grams to ounce conversion
6MTQHC	Grams to ounce conversion
6XUBJJ	grams to ounce conversion
7HDKDP	grams to ounce conversion
7Q8P8Q	grams to ounce conversion
7XHAQJ	grams to ounce conversion
84UA8D	grams to ounce conversion
8AWL3B	grams to ounce conversion
8Q7ENT	grams to ounce conversion
9RWZUN	grams to ounce conversion
9WB7YB	grams to ounce conversion
AL337X	grams to ounce conversion
APKHAX	grams to ounce conversion
B83YXC	grams to ounce conversion
BEHJY4	grams to ounce conversion
BHZGTL	grams to ounce conversion
CAKFT3	grams to ounce conversion
CRPM96	grams to ounce conversion
DQMCP7	grams to ounce conversion
ETRARM	grams to ounce conversion
F3CZRJ	grams to ounce conversion
FCDKRQ	grams to ounce conversion

TABLE 1

Question 18 - Internet History	
WebCode	**Response**
FFWFVJ	grams to ounce conversion
FJHEUY	free bookkeeping application
GBC7GA	grams to ounce conversion
GDR6K2	grams to ounce conversion
GNPA6M	grams to ounce conversion
GYL92Y	grams to ounce conversion
HPXMMN	grams to ounce conversion
HXQXXJ	grams to ounce conversion
J69MWJ	grams to ounce conversion
JYHDML	grams to ounce conversion
KAXHF3	Grams to ounce conversion
KGEDVW	grams to ounce conversion
MN787Z	grams to ounce conversion
N34LXG	grams to ounce conversion
N6PKXX	grams to ounce conversion
N9RLXU	grams to ounce conversion
NAGYFD	grams to ounce conversion
PAWF9K	grams to ounce conversion
RUGWR6	grams to ounce conversion
UR36WT	grams to ounce conversion
VKGQ9D	grams to ounce conversion
VXNLJ4	grams to ounce conversion
W94QCK	grams to ounce conversion
WAU23D	grams to ounce conversion
WDTCYD	grams to ounce conversion
WZ8ZM4	grams to ounce conversion
X78YBX	free bookkeeping application
XV7BJ2	grams to ounce conversion
YMTMH8	grams to ounce conversion
YUUYE6	grams to ounce conversion

TABLE 1

Question 18 - Internet History	
WebCode	**Response**
Z6A48L	grams to ounce conversion
Z8YEXE	grams to ounce conversion
ZJRXE7	grams to ounce conversion

Question 18: What was the last term searched using the Mozilla Firefox search engine?

Consensus Result: grams to ounce conversion

Expected Response Explanation:

Information regarding the last term searched using Mozilla is located here:
userdata (ExtX)/Root/data/org.mozilla.firefox/files/mozilla/k6cngp3n.default/browser.db
Table: history

Expected Response Illustration:

Mozilla Firefox search information:

Timestamp	Value	Source
11/28/2018 03:04 PM(UTC-5)	grams to ounce conversion	Mozilla Firefox

TABLE 1

Question 19 - Internet History

Question 19: How many PDF documents were downloaded using the Chrome search engine?

Manufacturer's Expected Response: Two (2)

WebCode	Response
26L4K9	2
2HT9U9	2
3DTGYG	Two (2)
4DUFQ6	2
4PYWYP	2
4WN9JF	2
4ZJ6ZT	2
64G4UJ	2
6MTQHC	2
6XUBJJ	6
7HDKDP	2
7Q8P8Q	2
7XHAQJ	2
84UA8D	2
8AWL3B	2
8Q7ENT	2
9RWZUN	Two
9WB7YB	2
AL337X	2
APKHAX	2
B83YXC	2
BEHJY4	Two(2)
BHZGTL	These are not services we provide as part of our analysis.
CAKFT3	2
CRPM96	2
DQMCP7	2
ETRARM	2
F3CZRJ	2
FCDKRQ	Two

TABLE 1

Question 19 - Internet History	
WebCode	**Response**
FFWFVJ	2
FJHEUY	two
GBC7GA	2
GDR6K2	2
GNPA6M	2
GYL92Y	2
HPXMMN	2
HXQXXJ	2
J69MWJ	2
JYHDML	2
KAXHF3	2
KGEDVW	2
MN787Z	6
N34LXG	2
N6PKXX	6
N9RLXU	2
NAGYFD	2
PAWF9K	2
RUGWR6	2
UR36WT	2
VKGQ9D	2
VXNLJ4	2
W94QCK	2
WAU23D	2
WDTCYD	2
WZ8ZM4	2
X78YBX	2
XV7BJ2	2
YMTMH8	2
YUUYE6	2

TABLE 1

Question 19 - Internet History	
WebCode	**Response**
Z6A48L	2
Z8YEXE	2
ZJRXE7	2

Question 19: How many PDF documents were downloaded using the Chrome search engine?

Consensus Result: Two (2)

Expected Response Explanation:

Information regarding documents downloaded using Chrome is located here:
userdata (ExtX)/Root/data/com.android.chrome/app_chrome/Default/History
Table: downloads_url_chains

Expected Response Illustration:

Chrome downloads:

	url
1	https://www.bcb.bm/media/134896/GENERAL_TERMS_AND_CONDITIONS_FINAL_Jul24_2017.pdf
2	https://www.bcb.bm/media/145615/FeeScheduleEffective20180501_UpdatedOn20180727.pdf
3	http://nextluxury.com/wp-content/uploads/male-with-cool-leg-celtic-owl-tattoo-design.jpg
4	https://i.pinimg.com/originals/21/b9/7b/21b97badc6224773b0f18553da6467fb.jpg
5	http://stylemann.com/wp-content/uploads/2016/11/3D-Tattoo-Designs-48-650x650.jpg
6	https://images.template.net/wp-content/uploads/2014/11/Tattoo-design-7.jpg

TABLE 1

Question 20 - Internet History

Question 20: How many pages were bookmarked on the Chrome search engine?

Manufacturer's Expected Response: Two (2)

WebCode	Response
26L4K9	4
2HT9U9	2
3DTGYG	Four (4)
4DUFQ6	2
4PYWYP	2
4WN9JF	2
4ZJ6ZT	2
64G4UJ	2
6MTQHC	2
6XUBJJ	2
7HDKDP	2
7Q8P8Q	2
7XHAQJ	2
84UA8D	4
8AWL3B	2
8Q7ENT	2
9RWZUN	Four
9WB7YB	2
AL337X	2
APKHAX	2
B83YXC	2
BEHJY4	Two(2)
BHZGTL	2
CAKFT3	2
CRPM96	2
DQMCP7	2
ETRARM	2
F3CZRJ	2
FCDKRQ	Two

TABLE 1

Question 20 - Internet History	
WebCode	**Response**
FFWFVJ	2
FJHEUY	two
GBC7GA	2
GDR6K2	2
GNPA6M	2
GYL92Y	2
HPXMMN	2
HXQXXJ	2
J69MWJ	2
JYHDML	2
KAXHF3	2
KGEDVW	2
MN787Z	4
N34LXG	2
N6PKXX	4
N9RLXU	2
NAGYFD	4
PAWF9K	2
RUGWR6	2
UR36WT	2
VKGQ9D	2
VXNLJ4	2
W94QCK	2
WAU23D	2
WDTCYD	2
WZ8ZM4	2
X78YBX	4
XV7BJ2	2
YMTMH8	2
YUUYE6	2

TABLE 1

Question 20 - Internet History	
WebCode	**Response**
Z6A48L	2
Z8YEXE	2
ZJRXE7	2

Question 20: How many pages were bookmarked on the Chrome search engine?

Consensus Result: Two (2)

Expected Response Explanation:

Information regarding pages bookmarked on Chrome is located here:
(ExtX)/Root/data/com.android.chrome/app_chrome/Default/History
Table: segments

Expected Response Illustration:

Chrome bookmarks:

#	Title	URL	Path	Timestamp	Source
1	Bernews - Bermuda's #1 sour...	http://bernews.com/	/Mobile bookmarks	11/27/2018 05:41 PM(UTC+0)	Chrome
2	Your Bermuda Banker, Everyw...	https://www.bcb.bm/	/Mobile bookmarks	11/27/2018 05:42 PM(UTC+0)	Chrome

Other Responses:

Eight participants reported a total of four (4) pages. This result may have been obtained by combining the total (2) under the chrome bookmarks and the total (2) within the "Synced data" folder.

TABLE 1

Question 21 - Media

Question 21: Provide the names of two pictures which were deleted. Separate answer with a comma(,)

Manufacturer's Expected Response: K2-Spice.jpg, Tattoo-design-7.jpg

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
26L4K9	000000000_999999.jpg, 12_task_thumbnail.png
2HT9U9	K2-Spice.jpg, Tatoo-design-7.jpg
3DTGYG	K2-Spice.jpg, Tattoo-design-7.jpg
4DUFQ6	K2-Spice.jpg, Tattoo-design-7.jpg
4PYWYP	000000000_999999.jpg , K2-Spice.jpg
4WN9JF	K2-Spice.jpg, Tattoo-design-7.jpg
4ZJ6ZT	K2-Spice.jpg, Tattoo-design-7.jpg
64G4UJ	K2-Spice.jpg, Tatto-design-7.jpg
6MTQHC	Tattoo-design-7.jpg, K2-spice.jpg
6XUBJJ	K2-Spice.jpg, Tattoo-design-7.jpg
7HDKDP	K2-Spice.jpg, Tattoo-design-7.jpg
7Q8P8Q	Tattoo-design-7.jpg, K2-Spice.jpg
7XHAQJ	K2-Spice.jpg,Screenshot_20181127-124936.jpg
84UA8D	K2-Spice.jpg, Tattoo-deswign-7.jpg
8AWL3B	K2-Spice.jpg, Tattoo-design-7.jpg
8Q7ENT	43_activity_icon_1543332711860.png, 43_activity_icon_1543332667680.png
9RWZUN	K2-Spice.jpg, Tattoo-design-7.jpg
9WB7YB	K2-Spice.jpg, Tattoo-design-7.jpg
AL337X	K2-Spice.jpg, Tattoo-design-7.jpg
APKHAX	K2-Spice.jpg, Tattoo-design-7.jpg
B83YXC	K2-Spice.jpg, Tattoo-design-7.jpg
BEHJY4	001497.JPEG,001501.JPEG
BHZGTL	K2-Spice.jpg, Tattoo-design-7.jpg
CAKFT3	K2-Spice.jpg, Tattoo-design-7.jpg
CRPM96	K2-Spice.jpg, Tattoo-design-7.jpg
DQMCP7	12_task_thumbnail.png, Tattoo-design-7.jpg
ETRARM	K2-spice.jpg, Tattoo-design-7.jpg
F3CZRJ	K2_Spice.jpg, Tattoo-design-7.jpg
FCDKRQ	Tattoo-design-7.jpg, K2-Spice.jpg

TABLE 1

Question 21 - Media	
WebCode	**Response** ** Inconsistencies not highlighted; No consensus achieved **
FFWFVJ	K2-Spice.jpg, Tattoo-design7.jpg
FJHEUY	K2-Spice.jpg, Tatto-design-7.jpg
GBC7GA	K2-Spice.jpg, Tattoo-design-7.jpg
GDR6K2	Tattoo-design-7.jpg, K2-Spice.jpg
GNPA6M	inode_1332EC800,inode_131F70500
GYL92Y	K2-Spice.jpg, Tattoo-design-7.jpg
HPXMMN	43_activity_icon_1543332667680.png, 43_activity_icon_1543332711860.png
HXQXXJ	K2-Spice.jpg, Screenshot_20181127-124936.png
J69MWJ	Tattoo-design-7.jpg, K2-Spice.jpg
JYHDML	77581c1ef7e45d9a_0_embedded_1.png, 000000000_999999.jpg
KAXHF3	K2-Spice.jpg, tattoo-design-7.jpg
KGEDVW	K2-Spice.jpg, Tattoo-design-7.jpg
MN787Z	43_activity_icon_1543332711860.png, 43_activity_icon_1543332667680.png
N34LXG	K2-Spice.jpg, Screenshot_20181127-124936.png
N6PKXX	43_activity_icon_1543332711860.png, 43_activity_icon_1543332667680.png
N9RLXU	Tattoo-design-7.jpg, K2-Spice.jpg
NAGYFD	K2-Spice.jpg, Tattoo-design-7.jpg
PAWF9K	K2-Spice.jpg ,Tattoo-design-7.jpg
RUGWR6	000000000_999999.jpg, K2-Spice.jpg
UR36WT	K2-Spice.jpg, Screenshot 20181127-124936.png
VKGQ9D	K2-Spice.jpg, Tattoo-design-7.jpg
VXNLJ4	K2-Spice, Tattoo-design-7
W94QCK	Screenshot_20181127-124936.png,K2-Spice.jpg
WAU23D	K2-Spice.jpg, Tattoo-design-7.jpg
WDTCYD	Screenshot_20181127-124936.png, Tatoo-design-7.jpg
WZ8ZM4	000000000_999999.jpg, 12_task_thumbnail.png
X78YBX	Screenshot_20181127-124936.png, Tattoo-design-7.jpg
XV7BJ2	43_activity_icon_1543332711860.png, 43_activity_icon_1543332711888.png
YMTMH8	icon.png, K2-Spice.jpg
YUUYE6	000000000_999999.jpg, 12_task_thumbnail.png

TABLE 1

Question 21 - Media		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
Z6A48L	K2-Spice.jpg, Tattoo-design-7.jpg	
Z8YEXE	K2-Spice.jpg, Tattoo-design-7.jpg	
ZJRXE7	K2-Spice.jpg, Tattoo-design-7.jpg	

Question 21: Provide the names of two pictures which were deleted. Separate answer with a comma(,)

Consensus Result: A consensus response was not achieved. The objective of this question was to identify which photos had been deleted from the downloaded files folder. Since the question did not specify that the deleted photos had to be ones that were downloaded to the phone, participants' results varied.

Expected Response Explanation:

The intention of this question was to have participants report only the deleted images that had been downloaded to the device, however due to the ambiguity of the question, participants could report two deleted images from a total of 20. Information regarding the deleted images from downloaded files is located at:
(ExtX)/Root/media/0/Download

Expected Response Illustration:

Downloaded images that were deleted:

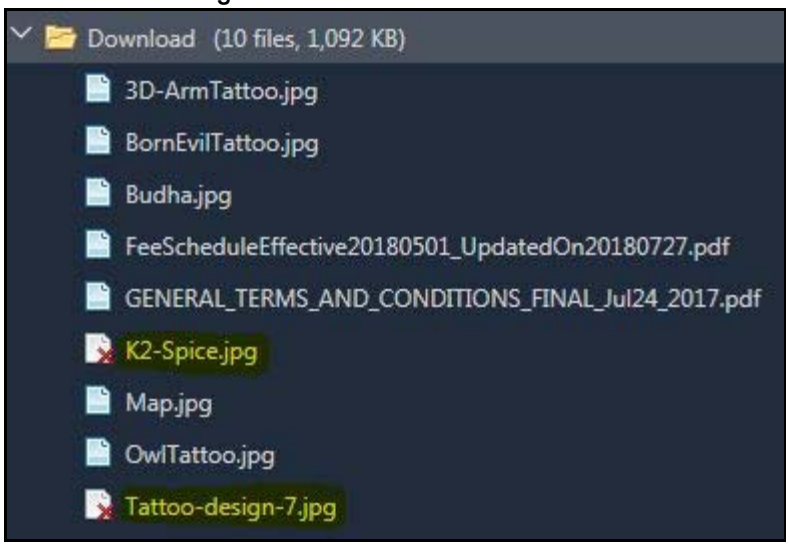


TABLE 1

Question 22 - Media

Question 22: How many pictures were taken using this camera? Do not include screenshots and downloads.

Manufacturer's Expected Response: Two (2)

WebCode	Response
26L4K9	2
2HT9U9	2
3DTGYG	Two (2)
4DUFQ6	2
4PYWYP	2
4WN9JF	2
4ZJ6ZT	2
64G4UJ	2
6MTQHC	2
6XUBJJ	2
7HDKDP	2
7Q8P8Q	2
7XHAQJ	2
84UA8D	2
8AWL3B	2
8Q7ENT	2
9RWZUN	Two
9WB7YB	2
AL337X	2
APKHAX	4
B83YXC	2
BEHJY4	Two(2)
BHZGTL	2
CAKFT3	2
CRPM96	2
DQMCP7	2
ETRARM	2
F3CZRJ	3

TABLE 1

Question 22 - Media	
WebCode	**Response**
FCDKRQ	Two Note: There are embedded versions of both images.
FFWFVJ	2
FJHEUY	two
GBC7GA	2
GDR6K2	2
GNPA6M	2
GYL92Y	2
HPXMMN	2
HXQXXJ	2
J69MWJ	2
JYHDML	2
KAXHF3	2
KGEDVW	2
MN787Z	2
N34LXG	2
N6PKXX	2
N9RLXU	2
NAGYFD	2
PAWF9K	2
RUGWR6	2
UR36WT	2
VKGQ9D	2
VXNLJ4	2
W94QCK	2
WAU23D	2
WDTCYD	2
WZ8ZM4	2
X78YBX	2
XV7BJ2	2
YMTMH8	2

TABLE 1

Question 22 - Media	
WebCode	**Response**
YUUYE6	2
Z6A48L	2
Z8YEXE	2
ZJRXE7	2

Question 22: How many pictures were taken using this camera? Do not include screenshots and downloads.

Consensus Result: Two (2)

Expected Response Explanation:

Information regarding pictures taken by this camera is located here:
userdata (ExtX)/Root/media/0/DCIM/Camera

Expected Response Illustration:

Camera information:

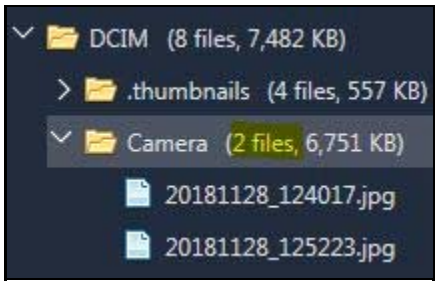


TABLE 1

Question 23 - Native Application

Question 23: What is the phone number of contact named "John Fuller"? Answer using the following format: 000-000-0000

Manufacturer's Expected Response: 703-544-6952

WebCode	Response
26L4K9	703-544-6952
2HT9U9	703-544-6952
3DTGYG	703-544-6952
4DUFQ6	703-544-6952
4PYWYP	703-544-6952
4WN9JF	703-544-6952
4ZJ6ZT	703-544-6952
64G4UJ	703-544-6952
6MTQHC	703-544-6952
6XUBJJ	703-544-6952
7HDKDP	703-544-6952
7Q8P8Q	703-544-6952
7XHAQJ	703-544-6952
84UA8D	703-544-6952
8AWL3B	703-544-6952
8Q7ENT	703-544-6952
9RWZUN	703-544-6952
9WB7YB	703-544-6952
AL337X	703-544-6952
APKHAX	703-544-6952
B83YXC	703-544-6952
BEHJY4	703-544-6952
BHZGTL	703-544-6952
CAKFT3	703-544-6952
CRPM96	703-544-6952
DQMCP7	703-544-6952
ETRARM	703-544-6952
F3CZRJ	703-544-6952

TABLE 1

Question 23 - Native Application	
WebCode	**Response**
FCDKRQ	703-544-6952
FFWFVJ	703-544-6952
FJHEUY	703-544-6952
GBC7GA	703-544-6952
GDR6K2	703-544-6952
GNPA6M	703-544-6952
GYL92Y	703-544-6952
HPXMMN	703-544-6952
HXQXXJ	703-544-6952
J69MWJ	703-544-6952
JYHDML	703-544-6952
KAXHF3	703-554-6952
KGEDVW	703-544-6952
MN787Z	(703) 544-6952
N34LXG	703-544-6952
N6PKXX	703-544-6952
N9RLXU	703-544-6952
NAGYFD	703-544-6952
PAWF9K	703-544-6952
RUGWR6	703-544-6952
UR36WT	703-544-6952
VKGQ9D	703-544-6952
VXNLJ4	703-544-6952
W94QCK	703-544-6952
WAU23D	703-544-6952
WDTCYD	703-544-6952
WZ8ZM4	703-544-6952
X78YBX	703-544-6952
XV7BJ2	703-544-6952
YMTMH8	703-544-6952

TABLE 1

Question 23 - Native Application	
WebCode	**Response**
YUUYE6	703-544-6952
Z6A48L	703-544-6952
Z8YEXE	703-544-6952
ZJRXE7	703-544-6952

Question 23: What is the phone number of contact named "John Fuller"? Answer using the following format: 000-000-0000

Consensus Result: 703-544-6952

Expected Response Explanation:

Information regarding contacts saved on this device can be found within the contacts2.db database file. This file is located at: /Root/data/com.android.providers.contacts/databases/contacts2.db-wal

Expected Response Illustration:

Contact information:

Name	Phones
John Fuller	(703) 544-6952

TABLE 1

Question 24 - Native Application

Question 24: Provide the epoch timestamp value of the last phone call placed to 703-544-6952.

Manufacturer's Expected Response: 1543424651904

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
26L4K9	1543434969000
2HT9U9	1543434969000
3DTGYG	1543406640
4DUFQ6	1543424651904
4PYWYP	1543424651904
4WN9JF	Wed, 28 November 2018 17:04:11.904 (UTC 0) Wed, 28 November 2018 12:04:11.904 (UTC -5)
4ZJ6ZT	1543424651000
64G4UJ	1543424651904
6MTQHC	01675B48B546
6XUBJJ	1543424651904
7HDKDP	1543424651000
7Q8P8Q	1543424651904
7XHAQJ	1543424651904
84UA8D	1543434969000
8AWL3B	11/28/2018 12:04:11 (UTC-5) 1543424651904
8Q7ENT	28.11.2018 17.04.11 (UTC+0)
9RWZUN	1543424640
9WB7YB	1543434969000
AL337X	1543428251
APKHAX	1543424651000
B83YXC	1543424651904
BEHJY4	1543434969000
BHZGTL	These are not services we provide as part of our analysis.
CAKFT3	1543424651904
CRPM96	1543424750918
DQMCP7	1543434969000
ETRARM	1543434969000
F3CZRJ	1543424651904
FCDKRQ	1543424651904

TABLE 1

Question 24 - Native Application		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
FFWFVJ	1543424640	
FJHEUY	1543424651904	
GBC7GA	1543424651904	
GDR6K2	1543424651904	
GNPA6M	1543424750918	
GYL92Y	1543424651904	
HPXMMN	1543406750	
HXQXXJ	1543434969000	
J69MWJ	12:04:11 PM(UTC-5)	
JYHDML	1543406651000	
KAXHF3	1543424651000	
KGEDVW	1543424651904	
MN787Z	1543424651	
N34LXG	1543424750000	
N6PKXX	1543424651	
N9RLXU	1543424651	
NAGYFD	1543424651904	
PAWF9K	28-Nov-18 12:04:11 PM(UTC-5) 1542560651	
RUGWR6	1543424651.904	
UR36WT	1543424651000	
VKGQ9D	1543424651904	
VXNLJ4	1543424651000	
W94QCK	1543424651904	
WAU23D	1543424651904	
WDTCYD	1543434969000	
WZ8ZM4	1543424640000	
X78YBX	1543424651904	
XV7BJ2	1543424640	
YMTMH8	"28-Nov-18 19:56:09" or "1543434969000"	
YUUYE6	1543424651904	

TABLE 1

Question 24 - Native Application		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
Z6A48L	1543424651	
Z8YEXE	1543434969	
ZJRXE7	1543424651000	

Question 24: Provide the epoch timestamp value of the last phone call placed to 703-544-6952.

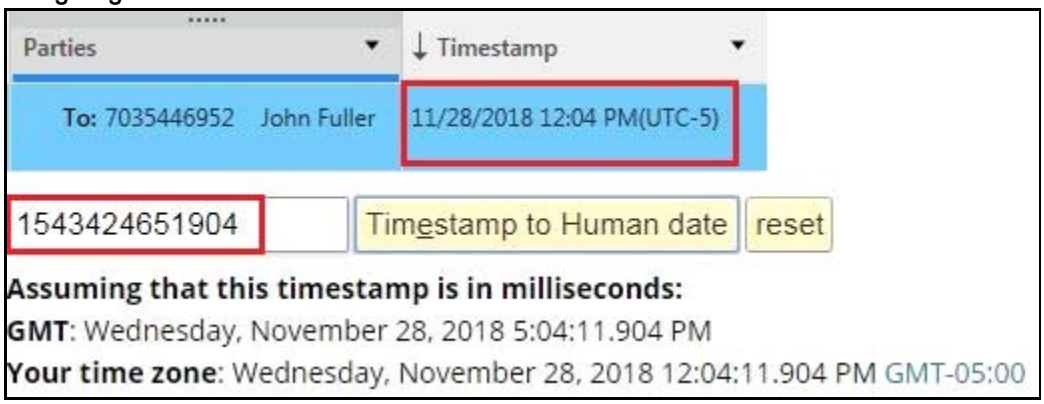
Consensus Result: No consensus was achieved. The objective of this question was to have participants identify the last call placed to a specified phone number, distinguishing outgoing calls from text messages or incoming calls.

Expected Response Explanation:

The expected response was 1543424651904.
Information regarding phone calls placed is located here:
userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db
Table: calls

Expected Response Illustration:

Outgoing calls information:



Other Responses:

The variety of responses reported by participants may have been due to the way the Calls table within the Contacts2 database was interpreted.

TABLE 1

Question 25 - Native Application

Question 25: To what phone number was the LAST call placed (outgoing) using this device? Provide the phone number in the following format: 000-000-0000

Manufacturer's Expected Response: 407-671-0983

WebCode	Response
26L4K9	703-544-6952
2HT9U9	703-544-6952
3DTGYG	407-671-0983
4DUFQ6	407-671-0983
4PYWYP	407-671-0983
4WN9JF	407-671-0983
4ZJ6ZT	407-671-0983
64G4UJ	407-671-0983
6MTQHC	407-671-0983
6XUBJJ	407-671-0983
7HDKDP	407-671-0983
7Q8P8Q	407-671-0983
7XHAQJ	407-671-0983
84UA8D	407-671-0983
8AWL3B	407-671-0983
8Q7ENT	407-671-0983
9RWZUN	407-671-0983
9WB7YB	407-671-0983
AL337X	407-671-0983
APKHAX	703-544-6952
B83YXC	407-671-0983
BEHJY4	703-544-6952
BHZGTL	407-671-0983
CAKFT3	407-671-0983
CRPM96	407-671-0983
DQMCP7	703-544-6952
ETRARM	703-544-6952
F3CZRJ	407-671-0983

TABLE 1

Question 25 - Native Application	
WebCode	**Response**
FCDKRQ	407-671-0983
FFWFVJ	407-671-0983
FJHEUY	407-671-0983
GBC7GA	407-671-0983
GDR6K2	407-671-0983
GNPA6M	407-671-0983
GYL92Y	407-671-0983
HPXMMN	407-671-0983
HXQXXJ	407-671-0983
J69MWJ	407-671-0983
JYHDML	407-671-0983
KAXHF3	407-671-0983
KGEDVW	407-671-0983
MN787Z	407-671-0983
N34LXG	407-671-0983
N6PKXX	407-671-0983
N9RLXU	407-671-0983
NAGYFD	407-671-0983
PAWF9K	407-671-0983
RUGWR6	407-671-0983
UR36WT	407-671-0983
VKGQ9D	407-671-0983
VXNLJ4	407-671-0983
W94QCK	407-671-0983
WAU23D	703-544-6952
WDTCYD	703-544-6952
WZ8ZM4	407-671-0983
X78YBX	407-671-0983
XV7BJ2	407-671-0983
YMTMH8	703-544-6952

TABLE 1

Question 25 - Native Application	
WebCode	**Response**
YUUYE6	407-671-0983
Z6A48L	407-671-0983
Z8YEXE	703-544-6952
ZJRXE7	703-544-6952

Question 25: To what phone number was the LAST call placed (outgoing) using this device? Provide the phone number in the following format: 000-000-0000

Consensus Result: 407-671-0983

Expected Response Explanation:

Information regarding the last outgoing call placed using this device is located here:
userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db-wal

Expected Response Illustration:

Outgoing call information:

#	Parties	Timestamp	Type	Source file information
1	To: 4076710983 Melissa Costa	11/28/2018 01:51 PM(UTC-5)	Outgoing	contacts2.db-wal : 0x2FCF84
2	To: 7035446952 John Fuller	11/28/2018 12:04 PM(UTC-5)	Outgoing	contacts2.db-wal : 0x2FD192
(2) 3	To: 5037632413 Dani Polanco	11/28/2018 11:02 AM(UTC-5)	Outgoing	contacts2.db-wal : 0x2FD2FB
4	To: 7035446952 John Fuller	11/28/2018 10:15 AM(UTC-5)	Outgoing	contacts2.db-wal : 0x2FD398
5	To: 7035446952 John Fuller	11/27/2018 09:42 AM(UTC-5)	Outgoing	contacts2.db-wal : 0x2FD4A6

Other Responses:

Eleven participants reported the phone number 703-544-6952; this number appears last in the contacts2 database however is not designated as a phone call but rather a message.

TABLE 1

Question 26 - Native Application

Question 26: How many outgoing calls were placed from this device? Do not include deleted calls.

Manufacturer's Expected Response: Five (5)

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
26L4K9	6
2HT9U9	8
3DTGYG	Five (5)
4DUFQ6	5
4PYWYP	5
4WN9JF	5
4ZJ6ZT	4
64G4UJ	5
6MTQHC	4
6XUBJJ	5
7HDKDP	4
7Q8P8Q	5
7XHAQJ	5
84UA8D	5
8AWL3B	5
8Q7ENT	4
9RWZUN	Five
9WB7YB	5
AL337X	5
APKHAX	3
B83YXC	5
BEHJY4	Six(6)
BHZGTL	4
CAKFT3	5
CRPM96	5
DQMCP7	7
ETRARM	4
F3CZRJ	5
FCDKRQ	Five

TABLE 1

Question 26 - Native Application		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
FFWFVJ	5	
FJHEUY	four	
GBC7GA	5	
GDR6K2	5	
GNPA6M	5	
GYL92Y	5	
HPXMMN	4	
HXQXXJ	5	
J69MWJ	5	
JYHDML	5	
KAXHF3	5	
KGEDVW	4	
MN787Z	5	
N34LXG	4	
N6PKXX	5	
N9RLXU	5	
NAGYFD	5	
PAWF9K	5	
RUGWR6	5	
UR36WT	5	
VKGQ9D	5	
VXNLJ4	5	
W94QCK	5	
WAU23D	5	
WDTCYD	7	
WZ8ZM4	5	
X78YBX	5	
XV7BJ2	5	
YMTMH8	7	
YUUYE6	5	

TABLE 1

Question 26 - Native Application		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
Z6A48L	5	
Z8YEXE	6	
ZJRXE7	Five (5)	

Question 26: How many outgoing calls were placed from this device? Do not include deleted calls.

Consensus Result: A consensus response was not achieved. The objective of this question was to have participants identify how many calls were placed from this phone, distinguishing outgoing calls from text messages or incoming calls.

Expected Response Explanation:

The expected response was Five (5).
Information regarding outgoing calls is located here:
userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db
Table: calls

Expected Response Illustration:

Outgoing call information:

#	Parties	↓ Timestamp	Type
1	To: 4076710983 Melissa Costa	11/28/2018 01:51 PM(UTC-5)	Outgoing
2	To: 7035446952 John Fuller	11/28/2018 12:04 PM(UTC-5)	Outgoing
3	To: 5037632413 Dani Polanco	11/28/2018 11:02 AM(UTC-5)	Outgoing
4	To: 7035446952 John Fuller	11/28/2018 10:15 AM(UTC-5)	Outgoing
5	To: 7035446952 John Fuller	11/27/2018 09:42 AM(UTC-5)	Outgoing

Other Responses:

Eighteen participants reported differing values from the expected response which may have been due to the way the Calls table within the Contacts2 database was interpreted.

TABLE 1

Question 27 - Native Application

Question 27: Provide the last term searched using Google Play Store.

Manufacturer's Expected Response: telegram

WebCode	Response
26L4K9	telegram
2HT9U9	telegram
3DTGYG	telegram
4DUFQ6	telegram
4PYWYP	telegram
4WN9JF	telegram
4ZJ6ZT	telegram
64G4UJ	Telegram
6MTQHC	telegram
6XUBJJ	telegram
7HDKDP	telegram
7Q8P8Q	telegram
7XHAQJ	telegram
84UA8D	telegram
8AWL3B	telegram
8Q7ENT	Telegram
9RWZUN	telegram
9WB7YB	Telegram
AL337X	telegram
APKHAX	telegram
B83YXC	telegram
BEHJY4	Telegram
BHZGTL	telegram
CAKFT3	telegram
CRPM96	telegram
DQMCP7	telegram
ETRARM	telegram
F3CZRJ	telegram
FCDKRQ	telegram

TABLE 1

Question 27 - Native Application	
WebCode	**Response**
FFWFVJ	telegram
FJHEUY	telegram
GBC7GA	telegram
GDR6K2	telegram
GNPA6M	telegram
GYL92Y	telegram
HPXMMN	telegram
HXQXXJ	telegram
J69MWJ	telegram
JYHDML	telegram
KAXHF3	Telegram
KGEDVW	telegram
MN787Z	Telegram
N34LXG	Telegram
N6PKXX	Telegram
N9RLXU	telegram
NAGYFD	telegram
PAWF9K	telegram
RUGWR6	telegram
UR36WT	telegram
VKGQ9D	Telegram
VXNLJ4	Telegram
W94QCK	telegram
WAU23D	telegram
WDTCYD	telegram
WZ8ZM4	telegram
X78YBX	telegram
XV7BJ2	telegram
YMTMH8	telegram
YUUYE6	Telegram

TABLE 1

Question 27 - Native Application	
WebCode	**Response**
Z6A48L	telegram
Z8YEXE	telegram
ZJRXE7	Telegram

Question 27: Provide the last term searched using Google Play Store.

Consensus Result: telegram

Expected Response Explanation:

Information regarding the last term searched using Google Play Store is located here:
userdata (ExtX)/Root/data/com.android.vending/databases/suggestions.db
Table: suggestions

Expected Response Illustration:

Google Play Store search terms:

	query	fx date
1	gmail	11/27/2018 01:32 PM
3	fir	11/27/2018 01:48 PM
4	evernote	11/27/2018 02:00 PM
5	telegram	11/27/2018 02:35 PM

TABLE 1

Question 28 - Native Application

Question 28: A calendar event was scheduled with a start date and time of 1544486400000. Provide the subject of the meeting.

Manufacturer's Expected Response: Shipment Pickup

WebCode	Response
26L4K9	Shipment Pickup
2HT9U9	Shipment Pickup
3DTGYG	Shipment Pickup
4DUFQ6	Shipment Pickup
4PYWYP	Shipment Pickup
4WN9JF	Shipment Pickup
4ZJ6ZT	Shipment Pickup
64G4UJ	Shipment Pickup
6MTQHC	Shipment Pickup
6XUBJJ	Shipment Pickup
7HDKDP	Shipment Pickup
7Q8P8Q	Shipment Pickup
7XHAQJ	Shipment Pickup
84UA8D	Shipment Pickup
8AWL3B	Shipment Pickup
8Q7ENT	Shipment Pickup
9RWZUN	Shipment Pickup
9WB7YB	Shipment Pickup
AL337X	Shipment Pickup
APKHAX	Shipment Pickup
B83YXC	Shipment Pickup
BEHJY4	Shipment Pickup
BHZGTL	These are not services we provide as part of our analysis.
CAKFT3	Shipment Pickup
CRPM96	Shipment Pickup
DQMCP7	Shipment Pickup
ETRARM	Shipment Pickup
F3CZRJ	Shipment Pickup

TABLE 1

Question 28 - Native Application	
WebCode	**Response**
FCDKRQ	Shipment Pickup
FFWFVJ	Shipment Pickup
FJHEUY	Shipment Pickup
GBC7GA	Shipment Pickup
GDR6K2	Shipment Pickup
GNPA6M	Shipment Pickup
GYL92Y	Shipment Pickup
HPXMMN	Shipment Pickup
HXQXXJ	Shipment Pickup
J69MWJ	Meeting with Tony
JYHDML	Shipment Pickup
KAXHF3	Shipment Pickup
KGEDVW	Shipment Pickup
MN787Z	Outside Leesburg Church
N34LXG	Shipment Pickup
N6PKXX	Shipment Pickup
N9RLXU	Shipment Pickup
NAGYFD	Shipment Pickup
PAWF9K	Title: Shipment Pickup
RUGWR6	Shipment Pickup
UR36WT	Shipment Pickup
VKGQ9D	Shipment Pickup
VXNLJ4	Shipment Pickup
W94QCK	Shipment Pickup
WAU23D	Shipment Pickup
WDTCYD	Shipment Pickup
WZ8ZM4	Shipment Pickup
X78YBX	Shipment Pickup
XV7BJ2	Shipment Pickup
YMTMH8	Shipment Pickup

TABLE 1

Question 28 - Native Application	
WebCode	**Response**
YUUYE6	Shipment Pickup
Z6A48L	Shipment Pickup
Z8YEXE	Shipment Pickup
ZJRXE7	Shipment Pickup

Question 28: A calendar event was scheduled with a start date and time of 1544486400000. Provide the subject of the meeting.

Consensus Result: Shipment Pickup

Expected Response Explanation:

Information regarding calendar events is located here:
userdata (ExtX)/Root/data/com.android.providers.calendar/databases/calendar.db
Table: Events

Expected Response Illustration:

Calendar Event information:

title	eventLocation	dtstart
Shipment Pickup	Outside Leesburg Church	1544486400000

TABLE 1

Question 29 - Third Party Application

Question 29: What is John Fuller's user ID (Party identifier) for the Telegram application?

Manufacturer's Expected Response: 706302018

WebCode	Response
26L4K9	706302018
2HT9U9	706302018
3DTGYG	706302018
4DUFQ6	706302018
4PYWYP	706302018
4WN9JF	706302018
4ZJ6ZT	706302018
64G4UJ	706302018
6MTQHC	706302018
6XUBJJ	706302018
7HDKDP	706302018
7Q8P8Q	706302018
7XHAQJ	706302018
84UA8D	706302018
8AWL3B	706302018
8Q7ENT	15719267559
9RWZUN	706302018
9WB7YB	706302018
AL337X	706302018
APKHAX	15719267559
B83YXC	706302018
BEHJY4	706302018
BHZGTL	706302018
CAKFT3	15719267559
CRPM96	706302018
DQMCP7	706302018
ETRARM	706302018
F3CZRJ	787961724
FCDKRQ	706302018

TABLE 1

Question 29 - Third Party Application	
WebCode	**Response**
FFWFVJ	15719267559
FJHEUY	John Fuller Telegram (15719267559)
GBC7GA	706302018
GDR6K2	706302018
GNPA6M	706302018
GYL92Y	706302018
HPXMMN	706302018
HXQXXJ	706302018
J69MWJ	15719267559
JYHDML	706302018
KAXHF3	706302018
KGEDVW	706302018
MN787Z	706302018
N34LXG	706302018
N6PKXX	706302018
N9RLXU	706302018
NAGYFD	706302018
PAWF9K	UID: 706302018 Phone number: 17035446952
RUGWR6	706302018
UR36WT	706302018
VKGQ9D	706302018
VXNLJ4	706302018
W94QCK	706302018
WAU23D	17035446952
WDTCYD	706302018
WZ8ZM4	15719267559
X78YBX	706302018
XV7BJ2	15719267559
YMTMH8	706302018
YUUYE6	706302018

TABLE 1

Question 29 - Third Party Application	
WebCode	**Response**
Z6A48L	706302018
Z8YEXE	706302018
ZJRXE7	706302018

Question 29: What is John Fuller's user ID (Party identifier) for the Telegram application?

Consensus Result: 706302018

Expected Response Explanation:

Information regarding the user ID for the Telegram application is located here:
/Root/data/org.telegram.messenger/files/cache4.db-wal
Table: users

Expected Response Illustration:

Telegram application user ID:

uid	name	status	data
706302018	john fuller;;;	1543598894	▯▯.WBP*▯K▯ ▯▯JohnFuller 17035446952I9▯▯s\
787961724	carlos diaz;;;	0	▯▯.|W▯.▯@$ ▯▯4CarlosDiaz 15719267559

Other Responses:

Another eight participants reported the number belonging to this device.

TABLE 1

Question 30 - Third Party Application

Question 30: Based on the conversation on the Telegram application, provide the name of the new supplier. (First Last)

Manufacturer's Expected Response: Joe Monzo

WebCode	Response
26L4K9	Joe Monzo
2HT9U9	Joe Monzo
3DTGYG	Joe Monzo
4DUFQ6	Joe Monzo
4PYWYP	Joe Monzo
4WN9JF	Joe Monzo
4ZJ6ZT	Joe Monzo
64G4UJ	Joe Monzo
6MTQHC	Joe Monzo
6XUBJJ	Joe Monzo
7HDKDP	Joe Monzo
7Q8P8Q	Joe Monzo
7XHAQJ	Joe Monzo
84UA8D	Joe Monzo
8AWL3B	Joe Monzo
8Q7ENT	Joe Monzo
9RWZUN	Joe Monzo
9WB7YB	Joe Monzo
AL337X	Joe Monzo
APKHAX	Joe Monzo
B83YXC	Joe Monzo
BEHJY4	Joe Monzo
BHZGTL	Joe Monzo
CAKFT3	Joe Monzo
CRPM96	Joe Monzo
DQMCP7	Joe Monzo
ETRARM	Joe Monzo
F3CZRJ	Joe Monzo

TABLE 1

Question 30 - Third Party Application	
WebCode	**Response**
FCDKRQ	Joe Monzo
FFWFVJ	Joe Monzo
FJHEUY	Joe Monzo
GBC7GA	Joe Monzo
GDR6K2	Joe Monzo
GNPA6M	Joe Monzo
GYL92Y	Joe Monzo
HPXMMN	Joe Monzo
HXQXXJ	Joe Monzo
J69MWJ	Joe Monzo
JYHDML	Joe Monzo
KAXHF3	Joe Monzo
KGEDVW	Joe Monzo
MN787Z	Joe Monzo
N34LXG	Joe Monzo
N6PKXX	Joe Monzo
N9RLXU	Joe Monzo
NAGYFD	Joe Monzo
PAWF9K	Joe Monzo
RUGWR6	Joe Monzo
UR36WT	Joe Monzo
VKGQ9D	Joe Monzo
VXNLJ4	Joe Monzo
W94QCK	Joe
WAU23D	Joe Monzo
WDTCYD	Joe Monzo
WZ8ZM4	Joe Monzo
X78YBX	Joe Monzo
XV7BJ2	Joe Monzo
YMTMH8	Carlos Diaz

TABLE 1

Question 30 - Third Party Application	
WebCode	**Response**
YUUYE6	Joe Monzo
Z6A48L	Joe Monzo
Z8YEXE	Joe Monzo
ZJRXE7	Joe Monzo

Question 30: Based on the conversation on the Telegram application, provide the name of the new supplier. (First Last)

Consensus Result: Joe Monzo

Expected Response Explanation:

Information regarding conversations using the Telegram application is located here:
/Root/data/org.telegram.messenger/files/cache4.db-wal

Expected Response Illustration:

Telegram application communication:

TABLE 1

Question 31 - Third Party Application

Question 31: What is the version of the Telegram Application that is installed on this device?

Manufacturer's Expected Response: 4.9.1

WebCode	Response
26L4K9	4.9.1
2HT9U9	4.9.1
3DTGYG	4.9.1
4DUFQ6	4.9.1
4PYWYP	4.9.1
4WN9JF	4.9.1
4ZJ6ZT	4.9.1
64G4UJ	4.9.1
6MTQHC	4.9.1
6XUBJJ	4.9.1
7HDKDP	4.9.1
7Q8P8Q	4.9.1
7XHAQJ	4.9.1
84UA8D	4.9.1
8AWL3B	4.9.1
8Q7ENT	4.9.1
9RWZUN	4.9.1
9WB7YB	4.9.1
AL337X	4.9.1
APKHAX	4.9.1
B83YXC	4.9.1
BEHJY4	4.9.1 (13613)
BHZGTL	4.9.1
CAKFT3	4.9.1
CRPM96	4.9.1
DQMCP7	4.9.1
ETRARM	4.9.1
F3CZRJ	4.9.1
FCDKRQ	4.9.1

TABLE 1

Question 31 - Third Party Application	
WebCode	**Response**
FFWFVJ	4.9.1
FJHEUY	4.9.1
GBC7GA	4.9.1
GDR6K2	4.9.1
GNPA6M	13613
GYL92Y	4.9.1
HPXMMN	4.9.1
HXQXXJ	4.9.1
J69MWJ	4.9.1
JYHDML	4.9.1
KAXHF3	4.9.1
KGEDVW	4.9.1
MN787Z	4.9.1
N34LXG	4.9.1
N6PKXX	4.9.1
N9RLXU	4.9.1
NAGYFD	4.9.1
PAWF9K	4
RUGWR6	4.9.1
UR36WT	4.9.1
VKGQ9D	4.9.1
VXNLJ4	4.9.1
W94QCK	4.9.1
WAU23D	4.9.1
WDTCYD	4.9.1
WZ8ZM4	4.9.1
X78YBX	4.9.1
XV7BJ2	4.9.1
YMTMH8	13613
YUUYE6	4.9.1

TABLE 1

Question 31 - Third Party Application	
WebCode	**Response**
Z6A48L	4.9.1
Z8YEXE	4.9.1
ZJRXE7	9.26.1.

Question 31: What is the version of the Telegram Application that is installed on this device?

Consensus Result: 4.9.1

Expected Response Explanation:

Information regarding installed applications can be found within the Android Manifest. The database can be found at: /Root/app/org.telegram.messenger-1/base.apk/AndroidManifest.xml

Expected Response Illustration:

Telegram application version:

TABLE 1

Question 32 - Third Party Application

Question 32: What is the package_name for the Whisper Application?

Manufacturer's Expected Response: sh.whisper

WebCode	Response
26L4K9	sh.whisper
2HT9U9	sh.whisper
3DTGYG	sh.whisper
4DUFQ6	sh.whisper
4PYWYP	sh.whisper
4WN9JF	sh.whisper
4ZJ6ZT	sh.whisper
64G4UJ	Sh.whisper
6MTQHC	sh.whisper
6XUBJJ	sh.whisper
7HDKDP	sh.whisper
7Q8P8Q	sh.whisper
7XHAQJ	sh.whisper
84UA8D	sh.whisper
8AWL3B	sh.whisper
8Q7ENT	sh.whisper
9RWZUN	sh.whisper
9WB7YB	sh.whisper
AL337X	sh.whisper
APKHAX	sh.whisper
B83YXC	sh.whisper
BEHJY4	sh.whisper
BHZGTL	sh.whisper
CAKFT3	sh.whisper
CRPM96	sh.whisper
DQMCP7	sh.whisper
ETRARM	sh.whisper
F3CZRJ	sh.whisper
FCDKRQ	sh.whisper

TABLE 1

Question 32 - Third Party Application	
WebCode	**Response**
FFWFVJ	sh.whisper
FJHEUY	Sh.whisper
GBC7GA	sh.whisper
GDR6K2	sh.whisper
GNPA6M	sh.whisper
GYL92Y	sh.whisper
HPXMMN	sh.whisper
HXQXXJ	sh.whisper
J69MWJ	sh.whisper
JYHDML	sh.whisper
KAXHF3	sh.whisper
KGEDVW	sh.whisper
MN787Z	Sh.whisper
N34LXG	sh.whisper
N6PKXX	sh.whisper
N9RLXU	sh.whisper
NAGYFD	sh.whisper
PAWF9K	sh.whisper
RUGWR6	sh.whisper
UR36WT	sh.whisper
VKGQ9D	sh.whisper-1
VXNLJ4	sh.whisper
W94QCK	sh.whisper
WAU23D	sh.whisper
WDTCYD	sh.whisper
WZ8ZM4	sh.whisper
X78YBX	sh.whisper-1/base.apk
XV7BJ2	sh-whisper-1
YMTMH8	sh.whisper
YUUYE6	sh.whisper

TABLE 1

Question 32 - Third Party Application	
WebCode	**Response**
Z6A48L	sh.whisper
Z8YEXE	sh.whisper
ZJRXE7	sh.whisper

Question 32: What is the package_name for the Whisper Application?

Consensus Result: sh.whisper

Expected Response Explanation:

Information regarding the package_name for the Whisper application is located here:
/Root/data/com.android.vending/databases/localappstate.db
Table: appstate

Expected Response Illustration:

Whisper application Package_Name:

Name	Version	Identifier
Whisper	9.26.1	sh.whisper

TABLE 1

Question 33 - Third Party Application

Question 33: Provide the date of when the Whisper Application was downloaded (purchased)? Answer using the time zone set on the device using the following format: Month/Date/Year (MM/DD/YYYY)

Manufacturer's Expected Response: 11/27/2018

WebCode	Response
26L4K9	11/27/2018
2HT9U9	11/27/2018
3DTGYG	11/27/2018
4DUFQ6	11/27/2018
4PYWYP	27/11/2018
4WN9JF	11/27/2018
4ZJ6ZT	11/27/2018
64G4UJ	11/27/2018
6MTQHC	11/27/2018
6XUBJJ	11/27/2018
7HDKDP	11/27/2018
7Q8P8Q	11/27/2018
7XHAQJ	11/27/2018
84UA8D	11/27/2018
8AWL3B	11/27/2018
8Q7ENT	11/27/2018
9RWZUN	11/27/2018
9WB7YB	11/27/2018
AL337X	11/27/2018
APKHAX	11/27/2018
B83YXC	11/27/2018
BEHJY4	11/27/2018
BHZGTL	11/27/2018
CAKFT3	11/27/2018
CRPM96	11/27/2018
DQMCP7	11/27/2018
ETRARM	11/27/2018
F3CZRJ	11/27/2018

TABLE 1

Question 33 - Third Party Application	
WebCode	**Response**
FCDKRQ	11/27/2018
FFWFVJ	11/27/2018 08:39(UTC-5)
FJHEUY	11/27/2018
GBC7GA	11/27/2018
GDR6K2	11/27/2018
GNPA6M	11/27/2018
GYL92Y	11/27/2018
HPXMMN	11/27/2018
HXQXXJ	11/27/2018 08:39(UTC-5)
J69MWJ	11/27/2018 8:39:13 AM(UTC-5
JYHDML	11/27/2018
KAXHF3	11/27/2018
KGEDVW	11/27/2018
MN787Z	11/27/2018
N34LXG	11/27/2018
N6PKXX	11/27/2018
N9RLXU	11/27/2018
NAGYFD	11/27/2018
PAWF9K	Nov/27/18
RUGWR6	11/27/2018
UR36WT	11/27/2018
VKGQ9D	11/27/2018
VXNLJ4	11/27/2018
W94QCK	11/27/2018
WAU23D	11/27/2018
WDTCYD	11/27/2018
WZ8ZM4	11/27/2018
X78YBX	11/27/2018 8:39:13 AM(UTC-5)
XV7BJ2	11/27/2018
YMTMH8	11/27/2018

TABLE 1

Question 33 - Third Party Application	
WebCode	**Response**
YUUYE6	11/27/2018
Z6A48L	11/27/2018
Z8YEXE	11/27/2018
ZJRXE7	27.11.2018.

Question 33: Provide the date of when the Whisper Application was downloaded (purchased)? Answer using the time zone set on the device using the following format: Month/Date/Year (MM/DD/YYYY)

Consensus Result: 11/27/2018 and all formatting styles which represent the same date.

Expected Response Explanation:

Information regarding the date in which the Whisper application was downloaded is located here:
/Root/data/com.android.vending/databases/localappstate.db
Table: appstate

Expected Response Illustration:

Application purchases:

Name	Version	Identifier	↓ Purchase Date
Whisper	9.26.1	sh.whisper	11/27/2018 08:39 AM(UTC-5)

TABLE 1

Question 34 - Third Party Application

Question 34: Provide the username associated with the Whisper Application?

Manufacturer's Expected Response: Trout_wow

WebCode	Response
26L4K9	Trout_wow
2HT9U9	Trout_wow
3DTGYG	Trout_wow
4DUFQ6	Trout_wow
4PYWYP	Trout_wow
4WN9JF	Trout_wow
4ZJ6ZT	Trout_wow
64G4UJ	Trout_wow
6MTQHC	Trout_wow
6XUBJJ	Trout_wow
7HDKDP	Trout_wow
7Q8P8Q	Trout_wow
7XHAQJ	Trout_wow
84UA8D	Trout_wow
8AWL3B	Trout_wow
8Q7ENT	Trout_wow
9RWZUN	Trout_wow
9WB7YB	Trout_wow
AL337X	Trout_wow
APKHAX	Trout_wow
B83YXC	Trout_wow
BEHJY4	Trout_wow
BHZGTL	Trout_wow
CAKFT3	Trout_wow
CRPM96	Trout_wow
DQMCP7	Trout_wow
ETRARM	Trout_wow
F3CZRJ	Trout_wow
FCDKRQ	Trout_wow

TABLE 1

Question 34 - Third Party Application	
WebCode	**Response**
FFWFVJ	Trout_wow
FJHEUY	Trout_wow
GBC7GA	Trout_wow
GDR6K2	Trout_wow
GNPA6M	Trout_wow
GYL92Y	Trout_wow
HPXMMN	Trout_wow
HXQXXJ	Trout_wow
J69MWJ	Trout_wow
JYHDML	Trout_wow
KAXHF3	Trout_wow
KGEDVW	Trout_wow
MN787Z	Trout_wow
N34LXG	Trout_wow
N6PKXX	Trout_wow
N9RLXU	Trout_wow
NAGYFD	Trout_wow
PAWF9K	Trout_wow
RUGWR6	Trout_wow
UR36WT	Trout_wow
VKGQ9D	Ice_Junky
VXNLJ4	Trout_wow
W94QCK	Trout_wow
WAU23D	Trout_wow
WDTCYD	Trout_wow
WZ8ZM4	Trout_wow
X78YBX	Trout_wow
XV7BJ2	Trout_wow
YMTMH8	Trout_wow
YUUYE6	Trout_wow

TABLE 1

Question 34 - Third Party Application	
WebCode	**Response**
Z6A48L	Trout_wow
Z8YEXE	Trout_wow
ZJRXE7	Trout_wow

Question 34: Provide the username associated with the Whisper Application?

Consensus Result: Trout_wow

Expected Response Explanation:

Information regarding the Whisper application is located here:
userdata (ExtX)/Root/data/sh.whisper/databases/c.db
Table: "m"

Expected Response Illustration:

Whisper application username:

Username	Service Type
Trout_wow	Whisper

TABLE 1

Question 35 - Third Party Application

Question 35: Provide the body of the last message sent using the Whisper Application. Do not abbreviate or condense your answer.

Manufacturer's Expected Response: Hey Buddy, I am here. Where are you?

WebCode	Response
26L4K9	Hey Buddy, I am here. Where are you?
2HT9U9	Hey Buddy, I am here. Where are you?
3DTGYG	Hey Buddy, I am here. Where are you?
4DUFQ6	Hey Buddy, I am here. Where are you?
4PYWYP	Hey Buddy, I am here. Where are you?
4WN9JF	Hey Buddy, I am here. Where are you?
4ZJ6ZT	Hey Buddy, I am here. Where are you?
64G4UJ	Hey Buddy. I am here. Where are you?
6MTQHC	Hey Buddy, I am here. Where are you?
6XUBJJ	Hey Buddy, I am here. Where are you?
7HDKDP	Hey Buddy, I am here. Where are you?
7Q8P8Q	Hey Buddy, I am here. Where are you?
7XHAQJ	Hey Buddy, I am here. Where are you?
84UA8D	Hey Buddy, I am here. Where are you?
8AWL3B	Hey Buddy, I am here. Where are you?
8Q7ENT	Hey Buddy, I am here. Where are you?
9RWZUN	"Hey Buddy, I am here. Where are you?"
9WB7YB	Hey Buddy, I am here. Where are you?
AL337X	Hey Buddy, I am here. Where are you?
APKHAX	Hey Buddy, I am here. Where are you?
B83YXC	Hey Buddy, I am here. Where are you?
BEHJY4	Hey Buddy, I am here. where are you?
BHZGTL	Hey Buddy, I am here. Where are you?
CAKFT3	Hey Buddy, I am here. Where are you?
CRPM96	Hey Buddy, I am here. Where are you?
DQMCP7	Hey Buddy, I am here. Where are you?
ETRARM	Hey Buddy, I am here. Where are you?
F3CZRJ	Hey Buddy, I am here. Where are you?

TABLE 1

Question 35 - Third Party Application	
WebCode	**Response**
FCDKRQ	Hey Buddy, I am here. Where are you?
FFWFVJ	Hey Buddy, I am here. Where are you?
FJHEUY	Hey Buddy, I am here. Where are you?
GBC7GA	Hey Buddy, I am here. Where are you?
GDR6K2	Hey Buddy, I am here. Where are you?
GNPA6M	Hey Buddy, I am here. Where are you?
GYL92Y	Hey Buddy, I am here. Where are you?
HPXMMN	Hey Buddy, I am here. Where are you?
HXQXXJ	Hey Buddy, I am here. Where are you?
J69MWJ	Hey Buddy, I am here. Where are you?
JYHDML	Hey Buddy, I am here. Where are you?
KAXHF3	Hey buddy, I am here. Where are you?
KGEDVW	Hey Buddy, I am here. Where are you?
MN787Z	Hey Buddy, I am here. Where are you?
N34LXG	Hey Buddy, I am here. Where are you?
N6PKXX	Hey Buddy, I am here. Where are you?
N9RLXU	Hey Buddy, I am here. Where are you?
NAGYFD	Hey Buddy, I am here. Where are you?
PAWF9K	Hey Buddy, I am here. Where are you?
RUGWR6	Hey Buddy, I am here. Where are you?
UR36WT	Hey Buddy, I am here. Where are you?
VKGQ9D	Hey Buddy, I am here. Where are you?
VXNLJ4	Hey buddy, I am here. Where are you?
W94QCK	Hey Buddy, I am here. Where are you?
WAU23D	Hey Buddy, I am here. Where are you?
WDTCYD	Hey Buddy, I am here. Where are you?
WZ8ZM4	Hey Buddy, I am here. Where are you?
X78YBX	Hey Buddy, I am here. Where are you?
XV7BJ2	Hey Buddy, I am here. Where are you?
YMTMH8	Hey Buddy, I am here. Where are you?

TABLE 1

Question 35 - Third Party Application	
WebCode	**Response**
YUUYE6	Hey Buddy, I am here. Where are you?
Z6A48L	Hey Buddy, I am here. Where are you?
Z8YEXE	Hey Buddy, I am here. Where are you?
ZJRXE7	Hey Buddy, I am here. Where are you?

Question 35: Provide the body of the last message sent using the Whisper Application. Do not abbreviate or condense your answer.

Consensus Result: Hey Buddy, I am here. Where are you?

Expected Response Explanation:

Information regarding the last message sent using the Whisper application is located here:
userdata (ExtX)/Root/data/sh.whisper/databases/c.db
Table: "m"

Expected Response Illustration:

Whisper application:

ts	text
11/27/2018 07:06 PM	Hi
11/29/2018 02:07 PM	Is the shipment ready
11/29/2018 02:21 PM	Its ready. When do you want to pick it up?
11/29/2018 02:23 PM	Let's meet tomorrow. I will send you the address in an email
11/29/2018 02:24 PM	Okay
11/29/2018 02:25 PM	Don't tell anyone about the meeting. I don't trust anyone
11/29/2018 02:26 PM	Did something happen?
11/29/2018 02:27 PM	Someone has been stealing my money
11/29/2018 02:28 PM	It's been short by $500 or more since the last 2-3 months
11/29/2018 02:29 PM	That's not good
11/29/2018 02:30 PM	Yeah man. I will talk to Fuller and find out who the mole is.
11/29/2018 02:31 PM	Okay, I will see you tomorrow then
11/29/2018 02:32 PM	See you
11/30/2018 05:19 PM	Hey Buddy, I am here. Where are you?

TABLE 1

Question 36 - Third Party Application

Question 36: Provide the username with whom the user had the most communication via the Whisper Application.

Manufacturer's Expected Response: Ice_Junky

WebCode	Response
26L4K9	Ice_Junky
2HT9U9	Ice_Junky
3DTGYG	Ice_Junky
4DUFQ6	Ice_Junky
4PYWYP	Ice_Junky
4WN9JF	Ice_Junky
4ZJ6ZT	Ice_Junky
64G4UJ	Ice_Junky
6MTQHC	Ice_Junky
6XUBJJ	Ice_Junky
7HDKDP	Ice_Junky
7Q8P8Q	Ice_Junky
7XHAQJ	Ice_Junky
84UA8D	Ice_Junky
8AWL3B	Ice_Junky
8Q7ENT	Ice_Junky
9RWZUN	John Fuller
9WB7YB	Ice_Junky
AL337X	Ice_Junky
APKHAX	Ice_Junky
B83YXC	Ice_Junky
BEHJY4	Ice_Junky
BHZGTL	Ice_Junky
CAKFT3	Ice_Junky
CRPM96	Ice_Junky
DQMCP7	Ice_Junky
ETRARM	Ice_Junky
F3CZRJ	Ice_Junky

TABLE 1

Question 36 - Third Party Application	
WebCode	**Response**
FCDKRQ	Ice_Junky
FFWFVJ	Ice_Junky
FJHEUY	Ice_Junky
GBC7GA	Ice_Junky
GDR6K2	Ice_Junky
GNPA6M	Ice_Junky
GYL92Y	Ice_Junky
HPXMMN	Ice_Junky
HXQXXJ	Ice_Junky
J69MWJ	Ice_Junky
JYHDML	Ice_Junky
KAXHF3	Ice_Junky
KGEDVW	Ice_Junky
MN787Z	Ice_Junky
N34LXG	Trout_wow
N6PKXX	Ice_Junky
N9RLXU	Ice_Junky
NAGYFD	Ice_Junky
PAWF9K	Ice_Junky
RUGWR6	Ice_Junky
UR36WT	Ice_Junky
VKGQ9D	Trout_wow
VXNLJ4	ICE_Junky
W94QCK	Ice_Junky
WAU23D	Ice_Junky
WDTCYD	Ice_Junky
WZ8ZM4	Ice_Junky
X78YBX	Ice_Junky
XV7BJ2	Ice_Junky
YMTMH8	Trout_wow

TABLE 1

Question 36 - Third Party Application	
WebCode	**Response**
YUUYE6	Ice_Junky
Z6A48L	Ice_Junky
Z8YEXE	Ice_Junky
ZJRXE7	Ice_Junky

Question 36: Provide the username with whom the user had the most communication via the Whisper Application.

Consensus Result: Ice_Junky

Expected Response Explanation:

Information regarding communication using the Whisper application is located here:
userdata (ExtX)/Root/data/sh.whisper/databases/c.db
Table: "c"

Expected Response Illustration:

Whisper application communication information:

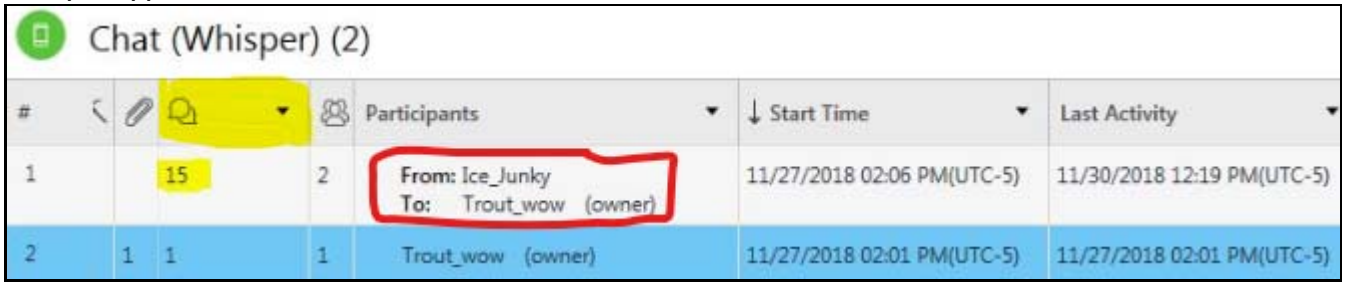


TABLE 1

Question 37 - Third Party Application

Question 37: Provide the title of the deleted note in the Evernote application.

Manufacturer's Expected Response: October Status

WebCode	Response
26L4K9	October Status
2HT9U9	October Status
3DTGYG	October Status
4DUFQ6	October Status
4PYWYP	October Status
4WN9JF	October Status
4ZJ6ZT	October Status
64G4UJ	October Status
6MTQHC	October Status
6XUBJJ	October Status
7HDKDP	October Status
7Q8P8Q	October Status
7XHAQJ	October Status
84UA8D	October Status
8AWL3B	October Status
8Q7ENT	October Status
9RWZUN	October Status
9WB7YB	October Status
AL337X	October Status
APKHAX	October Status
B83YXC	October Status
BEHJY4	October Status
BHZGTL	October Status
CAKFT3	October Status
CRPM96	October Status
DQMCP7	October Status
ETRARM	October Status
F3CZRJ	October Status
FCDKRQ	October Status

TABLE 1

Question 37 - Third Party Application	
WebCode	**Response**
FFWFVJ	October Status
FJHEUY	October Status
GBC7GA	October Status
GDR6K2	October Status
GNPA6M	October Status
GYL92Y	October Status
HPXMMN	October Status
HXQXXJ	October Status
J69MWJ	October Status
JYHDML	October Status
KAXHF3	October status
KGEDVW	October Status
MN787Z	October Status
N34LXG	October Status
N6PKXX	October Status
N9RLXU	October Status
NAGYFD	October Status
PAWF9K	October Status
RUGWR6	October Status
UR36WT	October Status
VKGQ9D	October Status
VXNLJ4	October Status
W94QCK	October Status
WAU23D	October Status
WDTCYD	October Status
WZ8ZM4	October Status
X78YBX	October Status
XV7BJ2	October Status
YMTMH8	October Status
YUUYE6	October Status

TABLE 1

Question 37 - Third Party Application	
WebCode	**Response**
Z6A48L	October Status
Z8YEXE	October Status
ZJRXE7	October Status

Question 37: Provide the title of the deleted note in the Evernote application.

Consensus Result: October Status

Expected Response Explanation:

Information regarding notes in the Evernote application is located here:
userdata (ExtX)/Root/data/com.evernote/files/user-196720852/.external-1543331602580-Evernote.db
Table: notes

Expected Response Illustration:

Evernote application deleted note:

Creation time	Modification Time	Title
11/27/2018 10:31 AM(UTC-5)	11/27/2018 10:31 AM(UTC...	October Status

TABLE 1

Question 38 - Third Party Application

Question 38: Provide the User ID associated with the third party application - 'Keeper Password Manager & Secure Vault'.

Manufacturer's Expected Response: diazcarlos1185@gmail.com

WebCode	Response
26L4K9	diazcarlos1185@gmail.com
2HT9U9	diazcarlos1185@gmail.com
3DTGYG	diazcarlos1185@gmail.com
4DUFQ6	diazcarlos1185@gmail.com
4PYWYP	diazcarlos1185@gmail.com
4WN9JF	diazcarlos1185@gmail.com
4ZJ6ZT	diazcarlos1185@gmail.com
64G4UJ	diazcarlos1185@gmail.com
6MTQHC	diazcarlos1185@gmail.com
6XUBJJ	diazcarlos1185@gmail.com
7HDKDP	diazcarlos1185@gmail.com
7Q8P8Q	diazcarlos1185@gmail.com
7XHAQJ	diazcarlos1185@gmail.com
84UA8D	diazcarlos1185@gmail.com
8AWL3B	diazcarlos1185@gmail.com
8Q7ENT	diazcarlos1185@gmail.com
9RWZUN	diazcarlos1185@gmail.com
9WB7YB	diazcarlos1185@gmail.com
AL337X	14205224
APKHAX	diazcarlos1185@gmail.com
B83YXC	diazcarlos1185@gmail.com
BEHJY4	diazcarlos1185@gmail.com
BHZGTL	_TqyFj50na44cjyA0u7ihw
CAKFT3	diazcarlos1185@gmail.com
CRPM96	diazcarlos1185@gmail.com
DQMCP7	diazcarlos1185@gmail.com
ETRARM	diazcarlos1185@gamil.com
F3CZRJ	diazcarlos1185@gmail.com

TABLE 1

Question 38 - Third Party Application	
WebCode	**Response**
FCDKRQ	diazcarlos1185@gmail.com
FFWFVJ	diazcarlos1185@gmail.com
FJHEUY	diazcarlos1185@gmail.com
GBC7GA	diazcarlos1185@gmail.com
GDR6K2	diazcarlos1185@gmail.com
GNPA6M	diazcarlos1185@gmail.com
GYL92Y	diazcarlos1185@gmail.com
HPXMMN	diazcarlos1185@gmail.com
HXQXXJ	diazcarlos1185@gmail.com
J69MWJ	diazcarlos1185@gmail.com
JYHDML	diazcarlos1185@gmail.com
KAXHF3	diazcarlos1185@gmail.com
KGEDVW	diazcarlos1185@gmail.com
MN787Z	diazcarlos1185@gmail.com
N34LXG	14205224 (diazcarlos1185@gmail.com)
N6PKXX	diazcarlos1185@gmail.com
N9RLXU	diazcarlos1185@gmail.com
NAGYFD	diazcarlos1185@gmail.com
PAWF9K	diazcarlos1185@gmail.com
RUGWR6	diazcarlos85@gmail.com
UR36WT	diazcarlos1185@gmail.com
VKGQ9D	diazcarlos1185@gmail.com
VXNLJ4	diazcarlos1185@gmail.com
W94QCK	14205224
WAU23D	diazcarlos1185@gmail.com
WDTCYD	diazcarlos1185@gmail.com
WZ8ZM4	diazcarlos1185@gmail.com
X78YBX	diazcarlos1185@gmail.com
XV7BJ2	diazcarlos1185@gmail.com
YMTMH8	id: "104" or "diazcarlos1185@gmail.com"

TABLE 1

Question 38 - Third Party Application	
WebCode	**Response**
YUUYE6	diazcarlos1185@gmail.com
Z6A48L	diazcarlos1185@gmail.com
Z8YEXE	diazcarlos1185@gmail.com
ZJRXE7	Keeper

Question 38: Provide the User ID associated with the third party application - 'Keeper Password Manager & Secure Vault'.

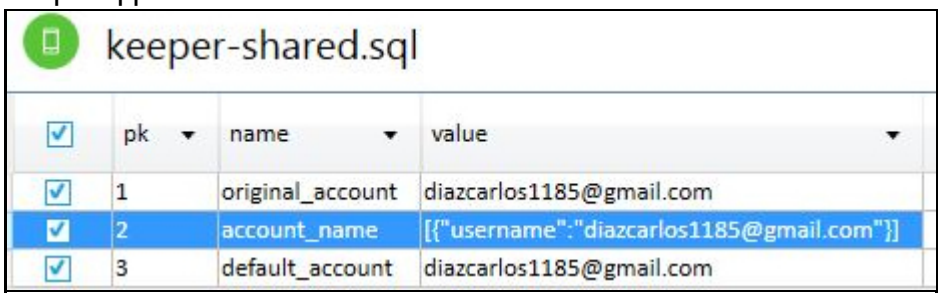
Consensus Result: diazcarlos1185@gmail.com

Expected Response Explanation:

Information regarding the User ID associated with the Keeper Password Manager & Secure Vault application is located here:
(ExtX)/Root/data/com.callpod.android_apps.keeper/databases/keeper-shared.sql

Expected Response Illustration:

Keeper application User ID:


keeper-shared.sql

	pk	name	value
☑	1	original_account	diazcarlos1185@gmail.com
☑	2	account_name	[{"username":"diazcarlos1185@gmail.com"}]
☑	3	default_account	diazcarlos1185@gmail.com

TABLE 1

Question 39 - Third Party Application

Question 39: Provide the account password associated with the third party application - 'Keeper Password Manager & Secure Vault'.

Manufacturer's Expected Response: password85

WebCode	Response
26L4K9	password85
2HT9U9	password85
3DTGYG	password85
4DUFQ6	password85
4PYWYP	password85
4WN9JF	password85
4ZJ6ZT	password85
64G4UJ	password85
6MTQHC	password85
6XUBJJ	password85
7HDKDP	password85
7Q8P8Q	password85
7XHAQJ	password85
84UA8D	password85
8AWL3B	password85
8Q7ENT	password85
9RWZUN	password85
9WB7YB	password85
AL337X	password85
APKHAX	password85
B83YXC	password85
BEHJY4	password85
BHZGTL	password85
CAKFT3	password85
CRPM96	password85
DQMCP7	password85
ETRARM	password85
F3CZRJ	password85

TABLE 1

Question 39 - Third Party Application	
WebCode	**Response**
FCDKRQ	password85
FFWFVJ	password85
FJHEUY	password85
GBC7GA	password85
GDR6K2	password85
GNPA6M	password85
GYL92Y	password85
HPXMMN	password85
HXQXXJ	password85
J69MWJ	password85
JYHDML	password85
KAXHF3	password85
KGEDVW	password85
MN787Z	password85
N34LXG	password85
N6PKXX	password85
N9RLXU	unknown
NAGYFD	password85
PAWF9K	password85
RUGWR6	password85
UR36WT	password85
VKGQ9D	password85
VXNLJ4	password85
W94QCK	password85
WAU23D	password85
WDTCYD	password85
WZ8ZM4	password85
X78YBX	password85
XV7BJ2	password85
YMTMH8	password85

TABLE 1

Question 39 - Third Party Application	
WebCode	**Response**
YUUYE6	password85
Z6A48L	password85
Z8YEXE	password85
ZJRXE7	password85

Question 39: Provide the account password associated with the third party application - 'Keeper Password Manager & Secure Vault'.

Consensus Result: password85

Expected Response Explanation:

Information regarding the account password associated with the Keeper Password Manager & Secure Vault application is located here: (ExtX)/Root/data/com.evernote/files/user-196720852/.external-1543331602580-Evernote.db
Tables: notes

Expected Response Illustration:

Evernote note containing Keeper application credentials:

#		Title	Body
1		Supplier's for December...	Willie - $4k Keith - $3k Sanchez - $5k Tony - $1k (new)
2		House Notes	First house at Lynn st - very small Second house at Church Hill Co
3		Keeper App credentials	ID: diazcarlos1185@gmail.com Password: password85
4		October Status	Joe's money sent 11/25 Others pending shipment
5	✖	October Status	Joe's money sent 11/25 Others pending shipment

TABLE 1

Question 40 - Third Party Application

Question 40: Did the User ID found within the 'Keeper Password Manager & Secure Vault' application database match with the User ID stored as notes in the Evernote application? Yes or No

Manufacturer's Expected Response: Yes

WebCode	Response
26L4K9	Yes
2HT9U9	Yes
3DTGYG	No
4DUFQ6	Yes
4PYWYP	No
4WN9JF	Yes
4ZJ6ZT	Yes
64G4UJ	Yes
6MTQHC	Yes
6XUBJJ	Yes
7HDKDP	Yes
7Q8P8Q	Yes
7XHAQJ	Yes
84UA8D	Yes
8AWL3B	Yes
8Q7ENT	No
9RWZUN	No
9WB7YB	Yes
AL337X	No
APKHAX	Yes
B83YXC	Yes
BEHJY4	Yes
BHZGTL	No
CAKFT3	Yes
CRPM96	Yes
DQMCP7	Yes
ETRARM	Yes
F3CZRJ	No

TABLE 1

Question 40 - Third Party Application	
WebCode	**Response**
FCDKRQ	Yes
FFWFVJ	No
FJHEUY	Yes
GBC7GA	Yes
GDR6K2	Yes
GNPA6M	Yes
GYL92Y	Yes
HPXMMN	Yes
HXQXXJ	No
J69MWJ	Yes
JYHDML	No
KAXHF3	Yes
KGEDVW	Yes
MN787Z	Yes
N34LXG	Yes. (No, if meaning the numeric ID)
N6PKXX	Yes
N9RLXU	Yes
NAGYFD	Yes
PAWF9K	Yes
RUGWR6	No
UR36WT	No
VKGQ9D	No
VXNLJ4	Yes
W94QCK	No
WAU23D	Yes
WDTCYD	Yes
WZ8ZM4	Yes
X78YBX	Yes
XV7BJ2	Yes
YMTMH8	Evernote: diazcarlos1185@gmail.com password: password85

TABLE 1

Question 40 - Third Party Application	
WebCode	**Response**
YUUYE6	Yes
Z6A48L	Yes
Z8YEXE	Yes
ZJRXE7	Yes

Question 40: Did the User ID found within the 'Keeper Password Manager & Secure Vault' application database match with the User ID stored as notes in the Evernote application? Yes or No

Consensus Result: Both responses Yes or No were accepted. This answer was dependent upon which table was viewed for the Keeper application.

Expected Response Explanation:

Information regarding the User ID used in the Keeper Password Manager & Secure Vault application and the User ID stored as a note are found at the following locations, respectively:
(ExtX)/Root/data/com.callpod.android_apps.keeper/databases/keeper-shared.sql
(ExtX)/Root/data/com.evernote/files/user-196720852/.external-1543331602580-Evernote.db

Expected Response Illustration:

Keeper User ID:

keeper-shared.sql

	pk	name	value
☑	1	original_account	diazcarlos1185@gmail.com
☑	2	account_name	[{"username":"diazcarlos1185@gmail.com"}]
☑	3	default_account	diazcarlos1185@gmail.com

Evernote information:

Title	Body
Keeper App credentials	ID: diazcarlos1185@gmail.com Password: password85

Other Responses:

Fourteen participants reported "No", possibly due how the settings table below from the Keeper application database was interpreted.

Settings table of the Keeper app:

diazcarlos1185@gmail.com.sql

Database view | Hex View | File Info

analytics_event	(3)
android_metadata	(1)
digital_asset_links	(0)
package_domain_mapping	(1)
password	(4)
recordLastGood	(0)
setting	(92)

pk	encrypted	cipher	name	setting_str	setting_int
51	0	0	email_address	diazcarlos1185@gmail.com	0
74	0	0	user_id		14205224

TABLE 1

Question 41 - Third Party Application

Question 41: How many records were saved in the Keeper Application?

Manufacturer's Expected Response: Four (4)

WebCode	Response
26L4K9	4
2HT9U9	4
3DTGYG	Four (4)
4DUFQ6	4
4PYWYP	4
4WN9JF	4
4ZJ6ZT	4
64G4UJ	4
6MTQHC	4
6XUBJJ	4
7HDKDP	4
7Q8P8Q	4
7XHAQJ	4
84UA8D	4
8AWL3B	4
8Q7ENT	4
9RWZUN	Four
9WB7YB	4
AL337X	4
APKHAX	4
B83YXC	4
BEHJY4	Four(4)
BHZGTL	4
CAKFT3	4
CRPM96	4
DQMCP7	4
ETRARM	4
F3CZRJ	4
FCDKRQ	Four

TABLE 1

Question 41 - Third Party Application	
WebCode	**Response**
FFWFVJ	4
FJHEUY	None
GBC7GA	4
GDR6K2	4
GNPA6M	4
GYL92Y	4
HPXMMN	4
HXQXXJ	4
J69MWJ	0
JYHDML	6
KAXHF3	4
KGEDVW	4
MN787Z	4
N34LXG	4
N6PKXX	4
N9RLXU	4
NAGYFD	4
PAWF9K	4
RUGWR6	4
UR36WT	4
VKGQ9D	40
VXNLJ4	4
W94QCK	4
WAU23D	4
WDTCYD	4
WZ8ZM4	4
X78YBX	32
XV7BJ2	
YMTMH8	4
YUUYE6	4

TABLE 1

Question 41 - Third Party Application	
WebCode	**Response**
Z6A48L	4
Z8YEXE	4
ZJRXE7	4

Question 41: How many records were saved in the Keeper Application?

Consensus Result: Four (4)

Expected Response Explanation:

Information regarding records saved in the Keeper application is located here:
userdata (ExtX)/Root/data/com.callpod.android_apps.keeper/databases/diazcarlos1185@gmail.com.sql

Expected Response Illustration:

Keeper application records:

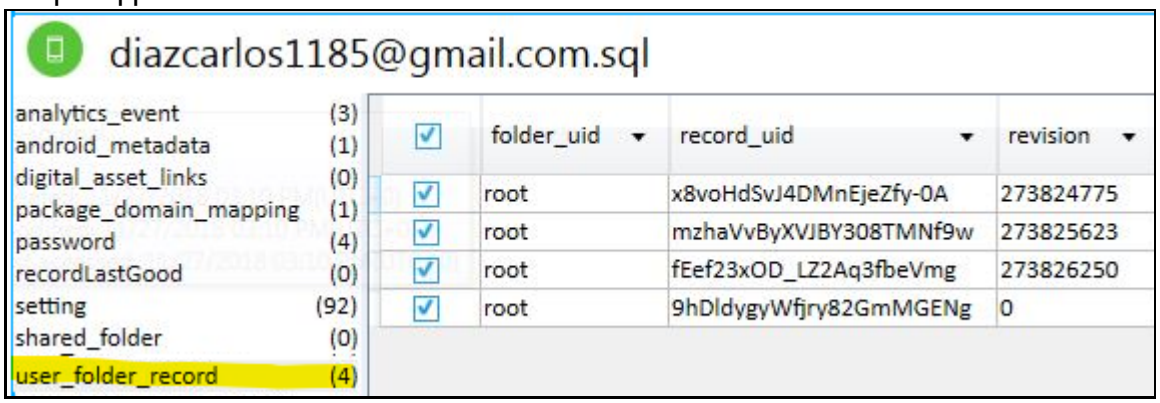


TABLE 1

Question 42 - Third Party Application

Question 42: Was the Waze application used to travel to 775 Gateway Dr SE, Leesburg, VA 20175? Yes or No

Manufacturer's Expected Response: No

WebCode	Response
26L4K9	Yes
2HT9U9	Yes
3DTGYG	Yes
4DUFQ6	No. The address was entered into the Waze application, but the Waze commands do not show driving commands to this location.
4PYWYP	No
4WN9JF	Yes
4ZJ6ZT	Yes
64G4UJ	Yes
6MTQHC	Yes
6XUBJJ	No
7HDKDP	Yes
7Q8P8Q	Yes
7XHAQJ	Yes
84UA8D	Yes
8AWL3B	Yes
8Q7ENT	No
9RWZUN	Yes
9WB7YB	Yes
AL337X	Yes
APKHAX	Yes
B83YXC	Yes
BEHJY4	Yes
BHZGTL	Yes
CAKFT3	Yes
CRPM96	Yes
DQMCP7	Yes
ETRARM	Yes
F3CZRJ	No

TABLE 1

Question 42 - Third Party Application	
WebCode	**Response**
FCDKRQ	No
FFWFVJ	No
FJHEUY	Yes
GBC7GA	Yes
GDR6K2	No
GNPA6M	Yes
GYL92Y	Yes
HPXMMN	Yes
HXQXXJ	Yes
J69MWJ	Yes
JYHDML	Yes
KAXHF3	Yes
KGEDVW	No
MN787Z	Yes
N34LXG	No
N6PKXX	Yes
N9RLXU	Yes
NAGYFD	Yes
PAWF9K	Yes
RUGWR6	No
UR36WT	Yes
VKGQ9D	No
VXNLJ4	No
W94QCK	Yes
WAU23D	No
WDTCYD	Yes
WZ8ZM4	Yes
X78YBX	Yes
XV7BJ2	Yes
YMTMH8	Yes

TABLE 1

Question 42 - Third Party Application	
WebCode	**Response**
YUUYE6	Yes
Z6A48L	Yes
Z8YEXE	No
ZJRXE7	Yes

Question 42: Was the Waze application used to travel to 775 Gateway Dr SE, Leesburg, VA 20175? Yes or No

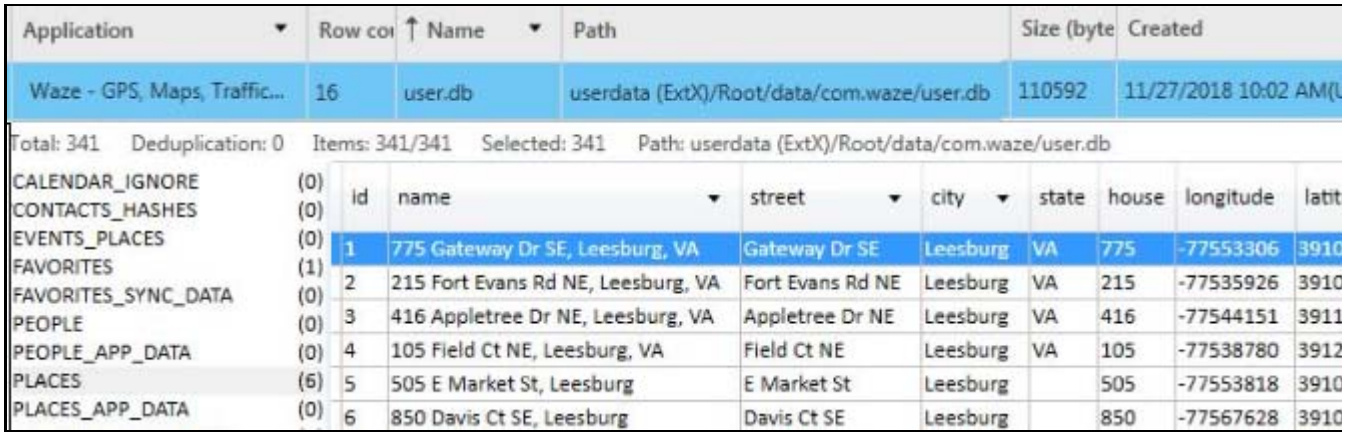
Consensus Result: Both responses No or Yes were accepted. The specified address was present in the Places table of the Waze application but was not shown in the Recents table.

Expected Response Explanation:

The address was entered into the Waze application causing it to be included in the Places table. However, in the Recents table this address was not shown to have been traveled to. The two tables are shown below. Information regarding addresses entered or traveled to using the Waze application are located here: userdata (ExtX)/Root/data/com.waze/user.db

Expected Response Illustration:

Waze - Places table:



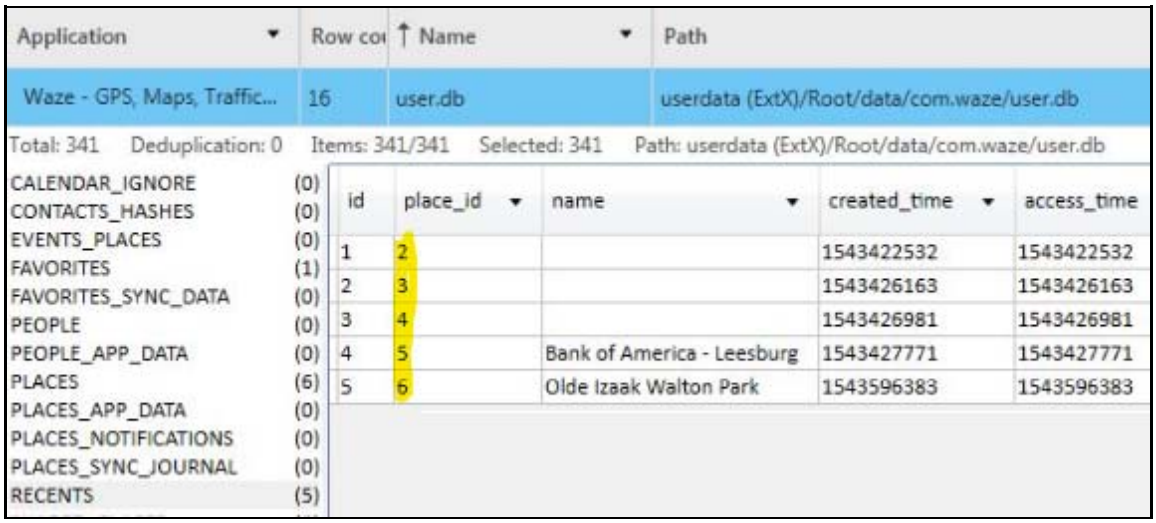
Application	Row co	Name	Path	Size (byte	Created
Waze - GPS, Maps, Traffic...	16	user.db	userdata (ExtX)/Root/data/com.waze/user.db	110592	11/27/2018 10:02 AM

Total: 341 Deduplication: 0 Items: 341/341 Selected: 341 Path: userdata (ExtX)/Root/data/com.waze/user.db

CALENDAR_IGNORE	(0)
CONTACTS_HASHES	(0)
EVENTS_PLACES	(0)
FAVORITES	(1)
FAVORITES_SYNC_DATA	(0)
PEOPLE	(0)
PEOPLE_APP_DATA	(0)
PLACES	(6)
PLACES_APP_DATA	(0)

id	name	street	city	state	house	longitude	latit
1	775 Gateway Dr SE, Leesburg, VA	Gateway Dr SE	Leesburg	VA	775	-77553306	3910
2	215 Fort Evans Rd NE, Leesburg, VA	Fort Evans Rd NE	Leesburg	VA	215	-77535926	3910
3	416 Appletree Dr NE, Leesburg, VA	Appletree Dr NE	Leesburg	VA	416	-77544151	3911
4	105 Field Ct NE, Leesburg, VA	Field Ct NE	Leesburg	VA	105	-77538780	3912
5	505 E Market St, Leesburg	E Market St	Leesburg		505	-77553818	3910
6	850 Davis Ct SE, Leesburg	Davis Ct SE	Leesburg		850	-77567628	3910

Waze - Recents table:



Application	Row co	Name	Path
Waze - GPS, Maps, Traffic...	16	user.db	userdata (ExtX)/Root/data/com.waze/user.db

Total: 341 Deduplication: 0 Items: 341/341 Selected: 341 Path: userdata (ExtX)/Root/data/com.waze/user.db

CALENDAR_IGNORE	(0)
CONTACTS_HASHES	(0)
EVENTS_PLACES	(0)
FAVORITES	(1)
FAVORITES_SYNC_DATA	(0)
PEOPLE	(0)
PEOPLE_APP_DATA	(0)
PLACES	(6)
PLACES_APP_DATA	(0)
PLACES_NOTIFICATIONS	(0)
PLACES_SYNC_JOURNAL	(0)
RECENTS	(5)

id	place_id	name	created_time	access_time
1	2		1543422532	1543422532
2	3		1543426163	1543426163
3	4		1543426981	1543426981
4	5	Bank of America - Leesburg	1543427771	1543427771
5	6	Olde Izaak Walton Park	1543596383	1543596383

TABLE 1

Question 43 - Third Party Application

Question 43: Provide the name of the last location this device traveled to using the Waze application.

Manufacturer's Expected Response: Olde Izaak Walton Park

WebCode	Response
26L4K9	Olde Izaak Walton Park
2HT9U9	850 Davis Ct SE, Leesburg
3DTGYG	Olde Izaak Walton Park
4DUFQ6	Olde Izaak Walton Park, located at 850 Davis Ct SE.
4PYWYP	Olde Izaak Walton Park, Davis Ct SE, 850, Leesburg
4WN9JF	850 davis Ct. SE, Leesburg Olde Izaak Walton Park
4ZJ6ZT	Olde Izaak Walton Park
64G4UJ	Olde Izaak Walton Park
6MTQHC	Olde Izaak Walton Park
6XUBJJ	Olde Izaak Walton Park
7HDKDP	Olde Izaak Walton Park
7Q8P8Q	850 Davis Ct SE, Leesburg
7XHAQJ	Olde Izaak Walton Park
84UA8D	Olde Izaak Walton Park, Davis Ct SE, 850 Leesburg
8AWL3B	Olde Izaak Walton Park
8Q7ENT	Olde Izaak Walton Park
9RWZUN	Olde Izaak Walton Park
9WB7YB	Olde Izaak Walton Park
AL337X	Olde Izaak Walton Park
APKHAX	Olde Izaak Walton Park
B83YXC	Olde Izaak Walton Park
BEHJY4	Olde Izaak Walton Park
BHZGTL	Olde Izaak Walton Park
CAKFT3	Olde Izaak Walton Park
CRPM96	Olde Izaak Walton Park
DQMCP7	Olde Izaak Walton Park 850 Davis Ct SE, Leesburg
ETRARM	Olde Izaak Walton Park
F3CZRJ	Davis Ct SE, 850, Leesburg
FCDKRQ	Olde Izaak Walton Park

TABLE 1

Question 43 - Third Party Application	
WebCode	**Response**
FFWFVJ	Olde Izaak Walton Park
FJHEUY	Olde Izaak Walton Park
GBC7GA	Davis Ct SE, 850, Leesburg
GDR6K2	Olde Izaak Walton Park
GNPA6M	Olde Izaak Walton Park
GYL92Y	Olde Izaak Walton Park
HPXMMN	Olde Izaak Walton Park
HXQXXJ	850 Davis Ct SE, Leesburg, VA 20175
J69MWJ	Olde Izaak Walton Park
JYHDML	Olde Izaak Walton Park
KAXHF3	Olde Izack Walton Park
KGEDVW	Olde Izaak Walton Park
MN787Z	850 Davis Ct SE, Leesburg
N34LXG	850 Davis Ct SE, LEESBURG.
N6PKXX	Olde Izaak Walton Park
N9RLXU	Olde Izaak Walton Park
NAGYFD	505 E Market St, Leesburg
PAWF9K	850 Davis Ct SE, Leesburg
RUGWR6	Olde Izaak Walton Park
UR36WT	Olde Izaak Walton Park
VKGQ9D	Olde Izaak Walton Park
VXNLJ4	Old Izaak Walton Park
W94QCK	Olde Izaak Walton Park
WAU23D	Olde Izaak Walton Park
WDTCYD	Olde Izaak Walton Park
WZ8ZM4	Olde Izaak Walton Park
X78YBX	850 Davis Ct SE, Leesburg
XV7BJ2	Davis Ct SE, 850, Leesburg
YMTMH8	Address: 850 Davis Ct SE, Leesburg Coordinates: 39.102417;-7.756762 Time stamp: 30-Nov-18 16:46:23 ID: venues.185074055.1850937158.1817986
YUUYE6	850 Davis Ct SE, Leesburg

TABLE 1

Question 43 - Third Party Application	
WebCode	**Response**
Z6A48L	Old Izaak Walton Park
Z8YEXE	850 Davis Ct SE, Leesburg
ZJRXE7	Sterling, Virginia 20166, USA

Question 43: Provide the name of the last location this device traveled to using the Waze application.

Consensus Result: "Olde Izaak Walton Park" and/or "850 Davis Ct SE, Leesburg" and all formatting styles which represent the same information.

Expected Response Explanation:

The information labeled as "Name" was different depending upon whether the Places table or the Recents table was accessed. Due to this both the address and location name were accepted for this question.
Information regarding the name of the last location traveled using the Waze application is located here:
userdata (ExtX)/Root/data/com.waze/user.db

Expected Response Illustration:

Recents table within the Waze application:

Path: userdata (ExtX)/Root/data/com.waze/user.db

CALENDAR_IGNORE	(0)
CONTACTS_HASHES	(0)
EVENTS_PLACES	(0)
FAVORITES	(1)
FAVORITES_SYNC_DATA	(0)
PEOPLE	(0)
PEOPLE_APP_DATA	(0)
PLACES	(6)
PLACES_APP_DATA	(0)
PLACES_NOTIFICATIONS	(0)
PLACES_SYNC_JOURNAL	(0)
RECENTS	(5)

name	created_time	access_time
	1543422532	1543422532
	1543426163	1543426163
	1543426981	1543426981
Bank of America - Leesburg	1543427771	1543427771
Olde Izaak Walton Park	1543596383	1543596383

Places table within the Waze application:

Path: userdata (ExtX)/Root/data/com.waze/user.db

CALENDAR_IGNORE	(0)
CONTACTS_HASHES	(0)
EVENTS_PLACES	(0)
FAVORITES	(1)
FAVORITES_SYNC_DATA	(0)
PEOPLE	(0)
PEOPLE_APP_DATA	(0)
PLACES	(6)
PLACES_APP_DATA	(0)

id	name	street	city	state	house
1	775 Gateway Dr SE, Leesburg, VA	Gateway Dr SE	Leesburg	VA	775
2	215 Fort Evans Rd NE, Leesburg, VA	Fort Evans Rd NE	Leesburg	VA	215
3	416 Appletree Dr NE, Leesburg, VA	Appletree Dr NE	Leesburg	VA	416
4	105 Field Ct NE, Leesburg, VA	Field Ct NE	Leesburg	VA	105
5	505 E Market St, Leesburg	E Market St	Leesburg		505
6	850 Davis Ct SE, Leesburg	Davis Ct SE	Leesburg		850

Additional Comments

TABLE 2

WebCode	Additional Comments
26L4K9	For Question 20 - 2 of the 4 bookmarks are duplicates.
4WN9JF	I think that this PT could be about 10 questions shorter.
4ZJ6ZT	It is unusual for us to interpret data while conducting casework. Our Laboratory provides the requested data and copies of it via a digital report for the submitting officer's review. Therefore, the submitting officer is left to interpret the data from the extraction(s). Additionally, regarding time stamps of files: we report out that which the file artifacts state.
64G4UJ	I like the Simple interface.
7HDKDP	It is unusual for us to interpret data while conducting casework. Our laboratory provides the requested data and copies of it via a digital report for the submitting officer's review. Therefore, the submitting officer is left to interpret the data from the extraction(s). Additionally, regarding time stamps of the files: we report out that which the file artifacts state.
84UA8D	The Bluetooth configuration (#9)was not answered because I could not find the answer. I don't believe that's an answerable question.
AL337X	A different model Samsung was used to load the image, because the exact model was unknown. The local time zone [country] is UTC-6, Time zone of the SIM was in UTC + 0, the time zone of the device is in UTC-5.
B83YXC	A few of the questions were confusing and I think it was the way they were worded.
BEHJY4	As the digital Forensics Field is increasing in complexity, especially in phone forensics, so more skills needed to increase our capabilities in analyzing and investigating in different cases
FFWFVJ	?
GDR6K2	Notes on a couple answers: Question 16: Three drugs were listed in body of email and one listed in the name of the email attachment. All four drug names included in answer. Question 42: The address in question is associated with the Waze app as a favorite location, but does not appear in recent locations. A favorite location can be entered by a user without using the app to travel to the location.
HXQXXJ	Question 40: In the app DB diazcarlos1185@gmail.com.sql in the setting table there is a row for the user_id. This user_id = 14205224 (int). Your questions can be interpreted in two ways. The user_id is the email address according to the Evernote entry, but in the Keeper DB the user_id is an interger and the email is the email address.
J69MWJ	Question 28 provides a start date and time of a calendar entry as 1544486400000. This number cannot be found in anything I attempt to look through.
N6PKXX	This test was not appropriate for a Practical testing situation and was poorly constructed.
N9RLXU	I have never had an investigator ask me for a date/time combination as an Epoch timestamp. They seem very popular with the creators of these tests, but I'm not sure how much real-world application those types of questions have.
UR36WT	There appeared to be several issues with this test. The keeper app's password while in an evernote did not decrypt the actual application. The number of possible items in it were found

TABLE 2

WebCode	Additional Comments
	in a db in an encrypted state. More concerning was the content of the group messages found within the w.db in the whisper app. While only a few items parsed while conducting a extensive exam a plethora of extremely hateful and offensive material was located. Was this known to be in the image?
W94QCK	Question 18: Mozilla Firefox is a browser, not a “search engine”. Question 19: Chrome is a browser, not a “search engine”. Question 20: Chrome is a browser, not a “search engine”
X78YBX	It appears - this phone belongs to a Carlos Diaz possible drug dealer. According to messages on the phone, Carlos was looking for a one way ticket to Bermuda via Reagan National airport (email - dated 11/28/18 to travelharmony.com) and set a meeting with John Fuller - to meet at Olde Izaak Walton Park on 11/30 12pm. The purpose for the meeting was to collect money that Carlos has been shorted from previous drug sales and find a possible mole in Carlos's orgainization. Fuller and Dani Polanco, appears to have have either set Carlos up to the police, or possibly been stealing money from Carlos as per Telegram messages. Carlos's safety should be concerning considering the intelligence gathered on the phone
Z6A48L	Some questions were poorly worded and not clear as to exactly what you are looking for. Regarding the Waze GPS question about traveling to an address, that address is listed as a favorite but that doesn't mean they actually went there. Maybe I was just unable to locate the artifacts that specify that the device actually traveled there, but if not this question needs to be clarified. Many of the questions were the types of questions that you would expect on an advanced certification test not a practical.

-End of Report-
(Appendix may follow)