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 - iOS Analysis
Test No. 20-5551 Summary Report

Participants were provided with data yielded from a logical extraction of an iPhone. They were asked to analyze the data and answer scenario based questions utilizing their own tools and methods. Data were returned from 87 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 – iOs Analysis test consisted of evidence data acquired from a smart phone in the .TAR file format. 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 case involving the ownership determination of a phone found after a protest demonstration, was created to generate user data on the evidence iPhone device. The execution of the scripted crime took place in between June and July of 2020. An iPhone 6s smart phone was used to perform the activities and generate the intended artifacts.

The phone data was acquired through a logical extraction of the smart phone utilizing Cellebrite software. Following sample validation, the phone data was converted into a .TAR compressed file. This file was 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 file.

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. Results from the predistribution laboratories were reviewed and certain questions were removed or rephrased as necessary.

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

The iPhone was recovered from lost and found after a protest demonstration in Washington, DC. A logical image of the iPhone was created and you have been tasked with analyzing the forensic image of this iPhone utilizing your own tools and methods. The extracted image has been provided to the examiner as abandoned property for the purpose of determining ownership information and reviewing the contents for any contact information for the owner, and any data of relevance to the examiner’s organization.

Manufacturer's Information, continued

Question	Manufacturer's Expected Response
1	What was the START date and time of the phone extraction? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM. *07/08/2020 09:01 PM*
2	Extract the .tar file from the downloaded .zip file and provide the SHA256 HASH for this .tar file. *1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79*
3	What method/type of extraction was performed? *Logical*
4	What is the version of extraction software used? *7.35.1.15*
5**	On what date was this device reset (erasing all content and settings)? Provide date in the following format: Month Day, Year. *June 9, 2020*
6	What is the model name of this phone (e.g. iPhone 4c)? *iPhone 6s*
7	What is the version of the operating system on this phone? *13.5.1*
8	What is the set time zone for this phone? Provide answer exactly as shown by the device. *America/New_York*
9	What is the ICCID number associated with this phone? *8901260063977237043*
10	Provide the Device Phone Number (MSISDN). *1-703-665-8672*
11	What is the language setting for this phone? *en-US*
12	Was icloud backup enabled? Provide a Yes/No response. *No*
13	Provide the AppleID associated with this phone. *jon.daniels39@icloud.com*
14	What is the SSID (name) of the LAST WiFi Hotspot connected to this phone? *MBR-f4b*

Manufacturer's Information, continued

Question	Manufacturer's Expected Response
15	Provide the BSSID of the WiFi Hotspot connected to this phone on 6/28/2020 at 12:52:33 PM (UTC-4)?
	0A:6C:6C:5E:B6:02
16	What is the make and model of the device with MAC Address 00:6A:8E:02:E9:2E?
	TaoTronics TT-BH041
17	What is the name of the user-installed (i.e. non-Apple) email app?
	ProtonMail
18	What is the version of the user-installed (i.e. non-Apple) email app?
	40.9.3
19	What is the email address associated with the user-installed (i.e. non-Apple) email app?
	jondaniel2020@protonmail.com
20	What is the email address associated with the native (i.e. Apple) email app?
	jon.daniels39@icloud.com
21	How many unique SMS messages were RECEIVED FROM the phone number associated with the contact listed as "Mark"?
	9
22	How many unique unread SMS messages are on the phone?
	6
23	Where did the device owner agree to meet on July 4?
	Lafayette Square
24	What contact (name) has the phone number "202-762-1401" listed as a "Pager" number in the iOS address book?
	James Roberts
25	What phone number did the phone miss a call from on June 24, 2020?
	12104087024
26	What contact (name) called the phone on July 4, 2020 at 6:31 PM?
	Mark
27	How many outgoing calls were made from this phone?
	5

Manufacturer's Information, continued

Question	*Manufacturer's Expected Response*
28	What was the date and time of the LAST outgoing call? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset). *07/04/2020 06:38 PM (UTC-4)*
29	With what service or application is the number 2029459404 associated? *TextNow*
30	What health-related app did the user install? *Renpho*
31	Describe the content of the file with MD5 Hash a17ff17faf23d3fa09b943c7b530d24f. *Rick Roll, Rick Astley, Never Gonna Give You Up, Music Video*
32	What is the address for the stored location in the Google Maps application? *21331 Gentry Dr, Sterling, VA 20166*
33	What location did the user search in Maps? *Monument avenue richmond*
34	Did the flash fire when taking the photo captured on 6/28/2020 at 12:57:10 PM(UTC-4)? Provide a Yes/No response. *No*
35	When did the user LAST visit news.google.com in the Safari browser? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset). *07/05/2020 01:07 PM (UTC-4)*
36	What type of payment card website did the user visit in the Chrome browser? *Prepaid reloadable debit, Vanilla, or My Vanilla*
37	What did the user create a reminder to do? *Backup phone*
38	When was the user scheduled to end his visit to DC? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset). *07/03/2020 07:59 PM(UTC-4)*
39	What are the location coordinates of the device on 6/28/2020 at 12:51:59 PM (UTC-4)? Provide your response using the following format: Latitude, Longitude. *37.558086, -77.467195*
40	Provide the content of a note created with the notes app. *Something noteworthy*

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 .tar file format, 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: phone and network settings, applications, communications, web browser history, and Geo-Location information.

Of the 40 questions, 39 reached a consensus when formatting differences and a few software tool-related variations were considered. Consensus was determined based on the total number of participants returning results per question. The question where a consensus was not achieved (#5) asked, "On what date was this device reset (erasing all content and settings)?". The majority of participants reported the expected response of June 9, 2020 however, since the time zone was not specified in the question and the phone was reset late at night, different time zones may have shown the reset occuring on the following day, June 10, 2020. Another subset of participants (21%) reported July 5, 2020, and the remainder of the population reported various other dates.

Please Note: Several forensic software tools were utilized during the validation of this test and may be referenced during the discussion of results. CTS does not endorse any particular tools.

Digital Evidence Responses

TABLE 1

Question 1

Question 1: What was the START date and time of the phone extraction? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM.

Manufacturer's Expected Response: 07/08/2020 09:01 PM

WebCode	Response
232E3H	07/08/2020 09:01 PM
23R6RY	07/08/2020 09:01 PM
2MP2LK	07/08/2020 09:01 PM (UTC -5)
2U4K6K	08/07/2020 09:01 PM
2UJ7EL	07/08/2020 09:01:51 PM
2ZD34D	07/08/2020 21:01:51pm
3LXYYV	7/8/2020 21:01 PM (UTC-5)
4KQATB	08/07/2020 21:01 PM
4VD9JG	07/08/2020 09:01 PM
6LKHCE	07/08/2020 09:01 PM
6R89XA	8.07.2020 09:01:51 pm
73ULRR	07/08/2020 09:01 PM
7FEZVR	07/08/2020 09:01 PM
7NZ8BH	07/08/2020 09:01 PM
7TZH7H	07/08/2020 09:01 PM
7WXYJC	07/08/2020 09:01:51 PM
82KA7F	07/08/2020 09:01 pm
8E9BN8	07/08/2020 21:01 PM
8FY44R	7/8/2020 9:01:51 PM
8XED4T	7/8/2020 9:01:51 PM
93EEZE	07/08/2020 09:01 PM
9AEVD6	07/08/2020, 09:01:51 PM
9C38CB	07/08/2020 09:01 PM
9J3RE7	07/08/2020 21:01:51
A8PRHD	07/08/2020 21:01 PM
AB3RE6	07/08/2020 09:01 PM
AJGDN9	07/08/2020 09:01 PM

TABLE 1

Question 1	
WebCode	**Response**
AUEEZC	07/08/2020 09:01 PM
B7LJQ6	07/08/2020 21:01 PM
BGDYWL	07/08/2020 21:01 PM
BK4CEC	07/08/2020 09:01 PM (UTC-5)
CMVPWM	07/08/2020 9:01 PM
CTTKD8	07/08/2020 09:01 PM
DDYEJ4	07/08/2020 09:01PM
DGXQF4	7/8/2020 9:01 PM
DJL3EA	7/8/2020 9:01 PM
EKZT67	08/07/2020 21:01 PM
ET7TE8	07/08/2020 21:01 PM
FNQKQ8	07/08/2020 09:01:51 PM
FXKMCH	07/08/2020 9:01 PM
G3E42G	7/8/2020 9:01:51 PM
GA8EUY	08/07/2020 21:01:51 PM
GJTH2X	07/08/2020 09:01 PM
GXBBQ6	07/08/2020 09:01 PM
HBTH3W	07/08/2020 09:01 PM
HRJN96	07/08/2020 09:01 PM
JRWEYZ	07/08/2020 09:01 PM
KQZJPW	07/08/2020 09:01 PM
L2Z97X	07/08/2020 21:01
L78WJY	07/08/2020 09:01 PM
LDRZQ3	07/08/2020 09:01 PM
LUED6U	07/08/2020 09:01 PM
MK4BJT	07/08/2020 09:01 p. m.
P94MFP	7/8/2020 9:01:51 PM
PBRYEU	07/08/2020 09:01 PM
PRFA2W	07/08/2020 21:01 PM
PVHA3U	07/08/2020 09:01 PM
PZYA29	07/08/2020 09:01 PM

TABLE 1

Question 1	
WebCode	**Response**
Q9J39W	07/08/2020 09:01 PM
QBL2JP	07/08/2020 21:01 PM
QTQBNV	7/8/2020 21:01
QZTKUN	08/07/2020 at 09:01 PM
RA9UVM	07/08/2020 09:01 PM
RWD889	07/08/2020 09:01:51 PM
T6DJYU	07/08/2020 09:01 PM
TGQJVM	07/08/2020 09:01:51 PM
TL2WDL	07/08/2020 9:01 PM
U2P8ZN	07/08/2020 09:01 PM
UCYFWG	START: 07/08/2020 9:01 PM, END: 07/08/2020 9:02 PM
UM9CJR	7/8/2020 9:01:51 PM
UPZBXQ	7/8/2020 9:01:51 PM
UQBAVK	07/08/2020 17:01 PM
UTYLUQ	07/08/2020 09:01:51 PM
V6M9DQ	7/8/2020 9:01 PM
VJC6V2	08/07/2020 21:01:51 (9:01:51 PM)
VU246Q	07/08/2020 09:01 PM
WJ3TAP	7/8/2020 9:01:51 PM
WX466N	07/08/2020 09:01 PM
X78WMG	7/08/2020 09:01 PM
X8ZRAP	07/08/2020 09:01PM
XJGCUL	07/08/2020 09:01 PM
XY9AWG	07/08/2020 9:01 PM EST (UTC -05:00)
XYELUY	7/8/2020 9:01:51 PM
YQ9AWF	07/08/2020 21:01PM or 9:01PM
Z8D34E	07/08/2020 9:01 PM
ZB38DY	07/08/2020 09:01:51 PM
ZX8VNE	07/08/2020 09:01 PM

TABLE 1

Question 1

Question 1: What was the START date and time of the phone extraction? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM.

Consensus Result: 07/08/2020 09:01 PM and all formatting styles including different time zones which represent the same information.

Expected Response Explanation:

This value is recorded by the acquisition tool and stored in the .ufd file.

Expected Response Illustration:

AppleDevice_AdvancedLogical.ufd

AppleDevice_AdvancedLogical.ufd

```
1  [Dumps]
2  FileDump=iPhoneBackup.tar
3  [FileDump]
4  Type=TARFolder
5  [SHA256]
6  iPhoneBackup.tar=1434EE7DC7A233A6452
7  [General]
8  ConnectionType=Cable No. 210
9  Date=08/07/2020 21:01:51
10 Device=IPHONE_BACKUP_LOGICAL
11 EndTime=08/07/2020 21:02:44
12 FullName=iPhone
13 ExtractionType=Logical
14 ExtractionMethod=iPhone 6s
15 Vendor=Apple
16 Model=iPhone 6s
17 UfdVer=1.1
18 Guid=446fd2fc-a492-4fcd-9a2c-54c2dc3
19 ExtractionSoftwareVersion=7.35.1.15
```

Cellebrite Extraction Summary

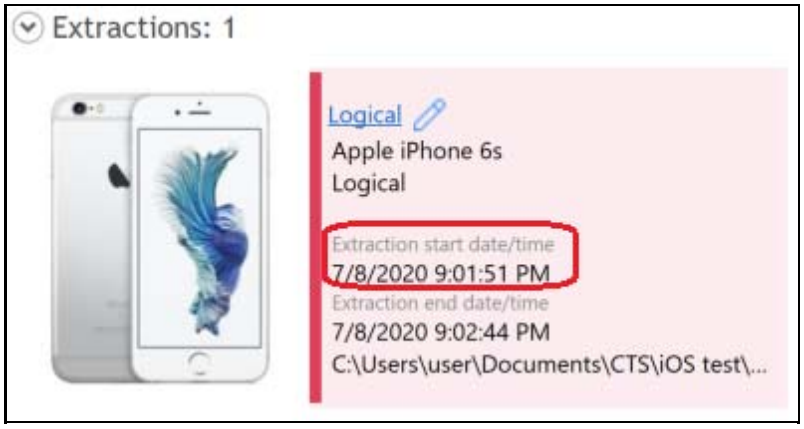


TABLE 1

Question 2

Question 2: Extract the .tar file from the downloaded .zip file and provide the SHA256 HASH for this .tar file.

Manufacturer's Expected Response: 1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79

WebCode	Response
232E3H	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
23R6RY	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
2MP2LK	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
2U4K6K	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
2UJ7EL	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
2ZD34D	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
3LXYYV	SHA256 1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
4KQATB	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
4VD9JG	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
6LKHCE	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
6R89XA	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
73ULRR	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
7FEZVR	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
7NZ8BH	SHA256: 1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
7TZH7H	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
7WXYJC	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
82KA7F	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
8E9BN8	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
8FY44R	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
8XED4T	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
93EEZE	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
9AEVD6	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
9C38CB	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
9J3RE7	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
A8PRHD	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
AB3RE6	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
AJGDN9	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
AUEEZC	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79

TABLE 1

Question 2	
WebCode	**Response**
B7LJQ6	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
BGDYWL	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
BK4CEC	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
CMVPWM	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
CTTKD8	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
DDYEJ4	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
DGXQF4	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
DJL3EA	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
EKZT67	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
ET7TE8	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
FNQKQ8	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
FXKMCH	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
G3E42G	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
GA8EUY	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
GJTH2X	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
GXBBQ6	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
HBTH3W	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
HRJN96	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
JRWEYZ	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
KQZJPW	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
L2Z97X	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
L78WJY	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
LDRZQ3	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
LUED6U	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
MK4BJT	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
P94MFP	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
PBRYEU	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F24BC79
PRFA2W	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
PVHA3U	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
PZYA29	SHA256: 1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
Q9J39W	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79

TABLE 1

Question 2	
WebCode	**Response**
QBL2JP	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
QTQBNV	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
QZTKUN	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
RA9UVM	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
RWD889	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
T6DJYU	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
TGQJVM	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
TL2WDL	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
U2P8ZN	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
UCYFWG	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
UM9CJR	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
UPZBXQ	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
UQBAVK	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
UTYLUQ	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
V6M9DQ	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
VJC6V2	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
VU246Q	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
WJ3TAP	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
WX466N	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
X78WMG	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
X8ZRAP	1434EE7DC7A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
XJGCUL	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79
XY9AWG	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
XYELUY	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
YQ9AWF	SHA-256 Hash 1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
Z8D34E	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
ZB38DY	1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79
ZX8VNE	1434ee7dc7a233a645250211975f17d50f3a90534d78f5e1baf66e14f242bc79

TABLE 1

Question 2

Question 2: Extract the .tar file from the downloaded .zip file and provide the SHA256 HASH for this .tar file.

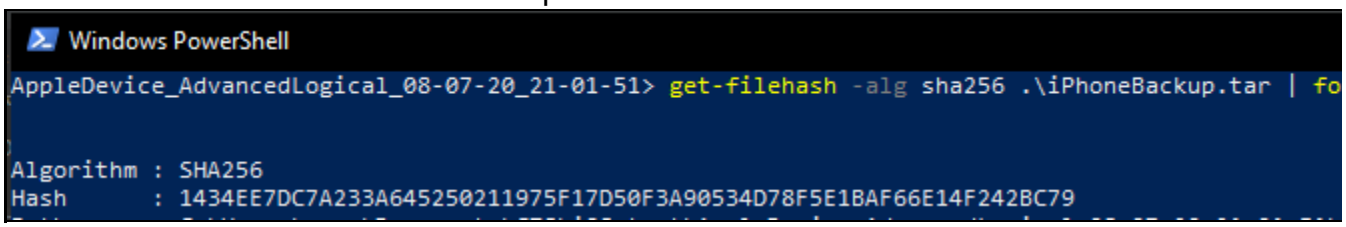
Consensus Result: 1434EE7DC7A233A645250211975F17D50F3A90534D78F5E1BAF66E14F242BC79

Expected Response Explanation:

Any reliable hashing tool can be used to calculate the SHA256 digest for the extracted file.

Expected Response Illustration:

PowerShell hash calculation of iPhoneBackup.tar



Linux sha256deep hash calculation of iPhoneBackup.tar

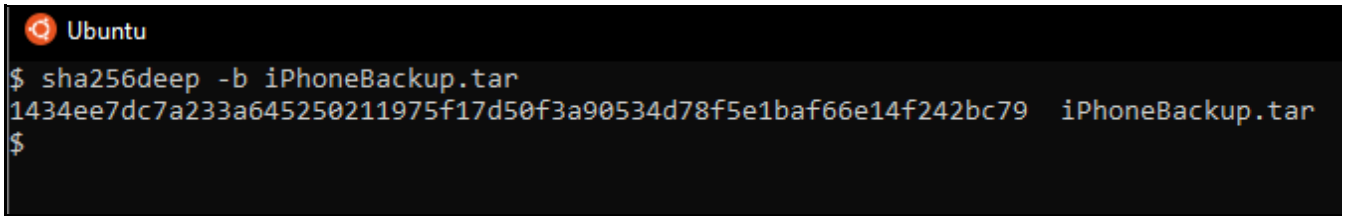


TABLE 1

Question 3

Question 3: What method/type of extraction was performed?

Manufacturer's Expected Response: Logical

WebCode	Response
232E3H	Logical
23R6RY	Logical
2MP2LK	Logical
2U4K6K	Logical
2UJ7EL	Logical
2ZD34D	Advanced Logical
3LXYYV	Logical extraction
4KQATB	Logical
4VD9JG	Logical
6LKHCE	Logical
6R89XA	Logical
73ULRR	Logical
7FEZVR	Logical
7NZ8BH	Logical
7TZH7H	LOGICAL
7WXYJC	Logical
82KA7F	Logical
8E9BN8	Advanced Logical
8FY44R	Logical
8XED4T	Logical
93EEZE	Logical
9AEVD6	ExtractionMethod=iPhone 6s, ExtractionType=Logical (AppleDevice_AdvancedLogical.ufd)
9C38CB	Logical
9J3RE7	Logical
A8PRHD	Logical
AB3RE6	Cellebrite Logical
AJGDN9	Apple Device Advanced Logical Extraction
AUEEZC	Logical
B7LJQ6	Logical

TABLE 1

Question 3	
WebCode	**Response**
BGDYWL	Logical
BK4CEC	Logical
CMVPWM	Logical
CTTKD8	Logical
DDYEJ4	Logical
DGXQF4	logical
DJL3EA	Logical
EKZT67	Logical
ET7TE8	Logical
FNQKQ8	Logical
FXKMCH	Advanced Logical method to obtain a Logical extraction.
G3E42G	ExtractionMethod=iPhone 6s/ExtractionType=Logical
GA8EUY	Logical
GJTH2X	A Logical extraction was performed.
GXBBQ6	iPhone 6s/Logical
HBTH3W	Logical
HRJN96	Logical/Advanced Logical
JRWEYZ	Logical
KQZJPW	Logical
L2Z97X	Advanced Logical according to Cellebrite Physical Analyzer, however the scenario lists it as a logical.
L78WJY	Logical
LDRZQ3	iPhone 6s Logical
LUED6U	Logical
MK4BJT	Logic
P94MFP	Logical
PBRYEU	Logical
PRFA2W	Logical
PVHA3U	Logical
PZYA29	Logical Extraction
Q9J39W	Logical
QBL2JP	Logical

TABLE 1

Question 3	
WebCode	**Response**
QTQBNV	Logical
QZTKUN	Logical
RA9UVM	Logical type
RWD889	Logical
T6DJYU	Logical
TGQJVM	Logical
TL2WDL	Logical
U2P8ZN	Logical
UCYFWG	Logical
UM9CJR	Logical
UPZBXQ	Logical
UQBAVK	Logical
UTYLUQ	Logical
V6M9DQ	Logical
VJC6V2	iPhone Backup Logical extraction
VU246Q	Logical
WJ3TAP	Logical
WX466N	Logical
X78WMG	Logical
X8ZRAP	Logical
XJGCUL	Logical
XY9AWG	Advanced Logical
XYELUY	Logical
YQ9AWF	Logical
Z8D34E	Logical
ZB38DY	Logical
ZX8VNE	Logical

TABLE 1

Question 3

Question 3: What method/type of extraction was performed?

Consensus Result: Logical

Expected Response Explanation:

This value is recorded by the acquisition tool and stored in the ufd file.

Expected Response Illustration:

AppleDevice_AdvancedLogical.ufd

AppleDevice_AdvancedLogical.ufd

```
[Dumps]
FileDump=iPhoneBackup.tar
[FileDump]
Type=TARFolder
[SHA256]
iPhoneBackup.tar=1434EE7DC7A233A64525021197
[General]
ConnectionType=Cable No. 210
Date=08/07/2020 21:01:51
Device=IPHONE_BACKUP_LOGICAL
EndTime=08/07/2020 21:02:44
FullName=iPhone
ExtractionType=Logical
ExtractionMethod=iPhone 6s
Vendor=Apple
Model=iPhone 6s
UfdVer=1.1
Guid=446fd2fc-a492-4fcd-9a2c-54c2dc332e49
ExtractionSoftwareVersion=7.35.1.15
IsEncrypted=True
```

Cellebrite Extraction Summary

TABLE 1

Question 4

Question 4: What is the version of extraction software used?

Manufacturer's
Expected Response: 7.35.1.15

WebCode	Response
232E3H	7.35.1.15
23R6RY	7.35.1.15
2MP2LK	7.35.1.15
2U4K6K	7.35.1.15
2UJ7EL	7.35.1.15
2ZD34D	7.35.1.15
3LXYYV	v. 7.35.1.15
4KQATB	7.35.1.15
4VD9JG	7.35.1.15
6LKHCE	7.35.1.15
6R89XA	7.35.1.15
73ULRR	7.35.1.15
7FEZVR	7.35.1.15
7NZ8BH	7.35.1.15
7TZH7H	7.35.1.15
7WXYJC	7.35.1.15
82KA7F	7.35.1.15
8E9BN8	7.35.1.15
8FY44R	7.35.1.15
8XED4T	7.35.1.15
93EEZE	7.35.1.15
9AEVD6	7.35.1.15
9C38CB	7.35.1.15
9J3RE7	7.35.1.15
A8PRHD	7.35.1.15
AB3RE6	7.35.1.15
AJGDN9	7.35.1.15
AUEEZC	7.35.1.15
B7LJQ6	7.35.1.15

TABLE 1

Question 4	
WebCode	**Response**
BGDYWL	7.35.1.15
BK4CEC	7.35.1.15
CMVPWM	7.35.1.15
CTTKD8	7.35.1.15
DDYEJ4	7.35.1.15
DGXQF4	7.35.1.15
DJL3EA	7.35.1.15
EKZT67	7.35.1.15
ET7TE8	7.35.1.15
FNQKQ8	7.35.1.15
FXKMCH	7.35.1.15
G3E42G	ExtractionSoftwareVersion=7.35.1.15
GA8EUY	7.35.1.15
GJTH2X	Extraction software version 7.35.1.15
GXBBQ6	7.35.1.15
HBTH3W	7.35.1.15
HRJN96	7.35.1.15
JRWEYZ	7.35.1.15
KQZJPW	7.35.1.15
L2Z97X	7.35.1.15
L78WJY	7.35.1.15
LDRZQ3	7.35.1.15
LUED6U	7.35.1.15
MK4BJT	7.35.1.15
P94MFP	7.35.1.15
PBRYEU	7.35.1.15
PRFA2W	7.35.1.15
PVHA3U	7.35.1.15
PZYA29	7.35.1.15
Q9J39W	7.35.1.15
QBL2JP	7.35.1.15

TABLE 1

Question 4	
WebCode	**Response**
QTQBNV	7.35.1.15
QZTKUN	7.35.1.15
RA9UVM	7.35.1.15
RWD889	7.35.1.15
T6DJYU	7.35.1.15
TGQJVM	7.35.1.15
TL2WDL	7.35.1.15
U2P8ZN	7.35.1.15
UCYFWG	7.35.1.15
UM9CJR	7.35.1.15
UPZBXQ	7.35.1.15
UQBAVK	7.35.1.15
UTYLUQ	7.35.1.15
V6M9DQ	7.35.1.15
VJC6V2	Software Version 7.35.1.15
VU246Q	7.35.1.15
WJ3TAP	7.35.1.15
WX466N	7.35.1.15
X78WMG	7.35.1.15
X8ZRAP	7.35.1.15
XJGCUL	7.35.1.15
XY9AWG	7.35.1.15
XYELUY	7.35.1.15
YQ9AWF	7.35.1.15
Z8D34E	7.35.1.15
ZB38DY	7.35.1.15
ZX8VNE	7.35.1.15

TABLE 1

Question 4

Question 4: What is the version of extraction software used?

Consensus Result: 7.35.1.15

Expected Response Explanation:

This value is recorded by the acquisition tool and stored in the .ufd file.

Expected Response Illustration:

AppleDevice_AdvancedLogical.ufd

AppleDevice_AdvancedLogical.ufd

```
[General]
ConnectionType=Cable No. 210
Date=08/07/2020 21:01:51
Device=IPHONE_BACKUP_LOGICAL
EndTime=08/07/2020 21:02:44
FullName=iPhone
ExtractionType=Logical
ExtractionMethod=iPhone 6s
Vendor=Apple
Model=iPhone 6s
UfdVer=1.1
Guid=446fd2fc-a492-4fcd-9a2c-54c2dc33
ExtractionSoftwareVersion=7.35.1.15
IsEncrypted=True
IsEncryptedBySystem=True
IsPartialData=False
BackupPassword=1234
```

TABLE 1

Question 5

Question 5: On what date was this device reset (erasing all content and settings)? Provide date in the following format: Month Day, Year.

Manufacturer's Expected Response: June 9, 2020

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
232E3H	June 9, 2020
23R6RY	06/09/2020
2MP2LK	The best guess is June 9, 2020, although the lack of a ".obliterated" file makes it harder to diagnose. - See comments regarding this answer.
2U4K6K	June 15 2020
2UJ7EL	July 5, 2020
2ZD34D	07/05/2020
3LXYYV	June 10,2020
4KQATB	June 9th, 2020
4VD9JG	June 9, 2020
6LKHCE	June 9, 2020
6R89XA	07.05.2020 14:58:40(UTC-4)
73ULRR	July 5, 2020
7FEZVR	June 9, 2020
7NZ8BH	June 9, 2020
7TZH7H	JUNE 09, 2020
7WXYJC	June 15, 2020
82KA7F	07/05,2020 (05-Jul-20 6:49:23 PM(UTC+0))
8E9BN8	07/05/2020
8FY44R	6/9/2020
8XED4T	6/09/2020
93EEZE	06/09/2020
9AEVD6	7/5/2020
9C38CB	06/09/2020
9J3RE7	06/15/2020
A8PRHD	June 9, 2020
AB3RE6	06/10/2020
AJGDN9	July 05, 2020
AUEEZC	June 9, 2020

TABLE 1

Question 5		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
B7LJQ6	06/09/2020	
BGDYWL	June 9, 2020	
BK4CEC	06/09/2020	
CMVPWM	06/09/2020	
CTTKD8	June 9, 2020	
DDYEJ4	June 10, 2020	
DGXQF4	6/9/2020	
DJL3EA	June 9, 2020	
EKZT67	June 09, 2020	
ET7TE8	07/05/2020	
FNQKQ8	July 5th, 2020	
FXKMCH	June 9, 2020	
G3E42G	June 5, 2020	
GA8EUY	June 9th, 2020	
GJTH2X	June 9th, 2020	
GXBBQ6	June 9, 2020	
HBTH3W	June 06, 2020	
HRJN96	June 05, 2020	
JRWEYZ	06/09/2020	
KQZJPW	June 09, 2020	
L2Z97X	June 9, 2020	
L78WJY	June 9th, 2020	
LDRZQ3	June 9, 2020	
LUED6U	There is evidence that indicates the device was reset on June 9, 2020 (06/09/2020). Multiple databases created indicate a creation date of 6/09/2020, such as Addressbook.SQlitedb, Cellularusage.db, CallHistory.Storedata, and Datausage.sqlite. There are also data that indicates user activity beginning on 6/15/2020, such as network data usage, SMS activity, and contact information. There is also com.apple.purplebuddy activity on 6/15/2020. This is a file that is used to store internal settings of an iPhone while an iPhone is being setup.	
MK4BJT	07/05/2020	
P94MFP	7/5/2020	
PBRYEU	Our lab does not offer this determination	
PRFA2W	July 05, 2020.	

TABLE 1

Question 5		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
PVHA3U	June 9, 2020	
PZYA29	June 9, 2020	
Q9J39W	June 9, 2020	
QBL2JP	07/09/2020	
QTQBNV	7/5/2020 (See note in comments) [Table 2: Additional Comments]	
QZTKUN	7/5/2020	
RA9UVM	07/08/2020	
RWD889	June 9, 2020	
T6DJYU	June 9, 2020	
TGQJVM	6/15/2020 4:49:20 AM (UTC-7)	
TL2WDL	06/09/2020	
U2P8ZN	June 9, 2020 or June 10, 2020	
UCYFWG	July 5, 2020	
UM9CJR	June 9, 2020	
UPZBXQ	July 8, 2020	
UQBAVK	06/15/2020	
UTYLUQ	06/15/2020	
V6M9DQ	The .obliterated file which includes the creation time stamp of when an iOS device is reset does not exist in this extraction. This file is not recovered during a logical extraction. It is suggested that June 9, 2020 was the device reset date based upon the creation time of the AddresBook.sqlitedb, CallHistory.storedata, and sms.db. If referring to Last Activation Time: July 5, 2020.	
VJC6V2	07/05/2020	
VU246Q	06/9/2020	
WJ3TAP	June 15, 2020	
WX466N	June 9, 2020	
X78WMG	6.09.2020	
X8ZRAP	June 09, 2020	
XJGCUL	June 9, 2020	
XY9AWG	06/09/2020	
XYELUY	June 9, 2020	
YQ9AWF	06/09/2020	
Z8D34E	6/9/2020	
ZB38DY	July 5, 2020	

TABLE 1

Question 5		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
ZX8VNE	Sometime prior to 06/09/2020	

Question 5: On what date was this device reset (erasing all content and settings)? Provide date in the following format: Month Day, Year.

Consensus Result: While a majority (59%) of respondents provided the expected response, a consensus was not achieved for this question. The objective of this question was for the participants to review the timeline of filesystem events on the device, and identify when certain key operating system files were created, indicating a device reset.

Expected Response Explanation:

Viewing the extracted files in both Cellebrite and Autopsy shows significant filesystem activity (and generation of new data and log files consistent with reset and use) on June 9, and no such activity prior to that time.

Expected Response Illustration:

Cellebrite Timeline view showing earliest Log Entries

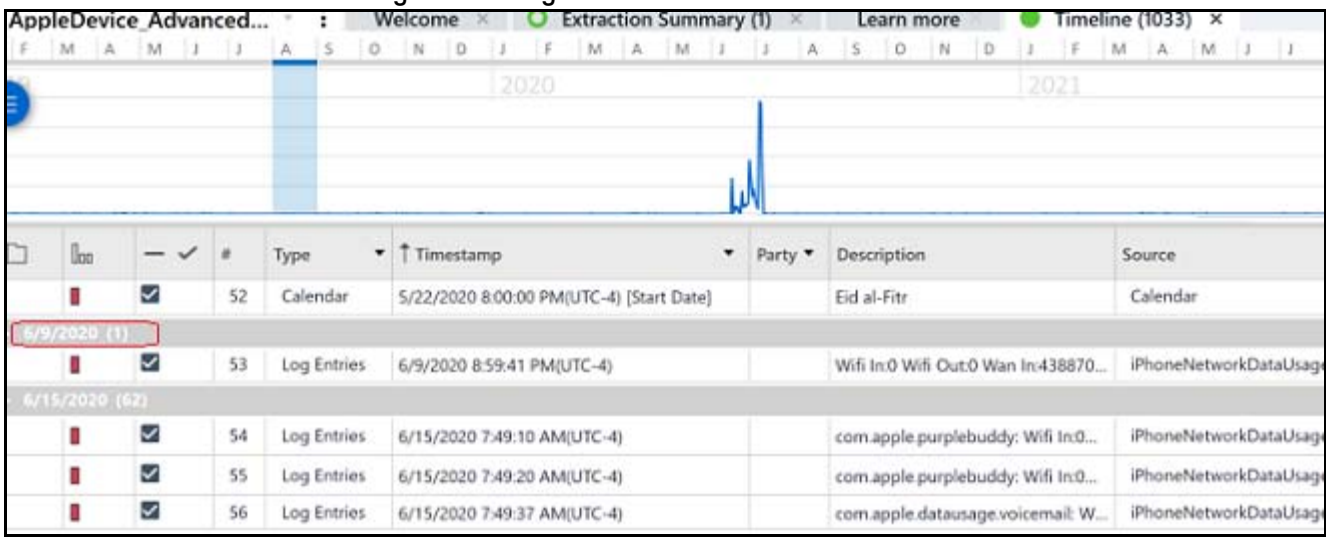


TABLE 1

Question 5

Autopsy Timeline view showing creation dates for various database files

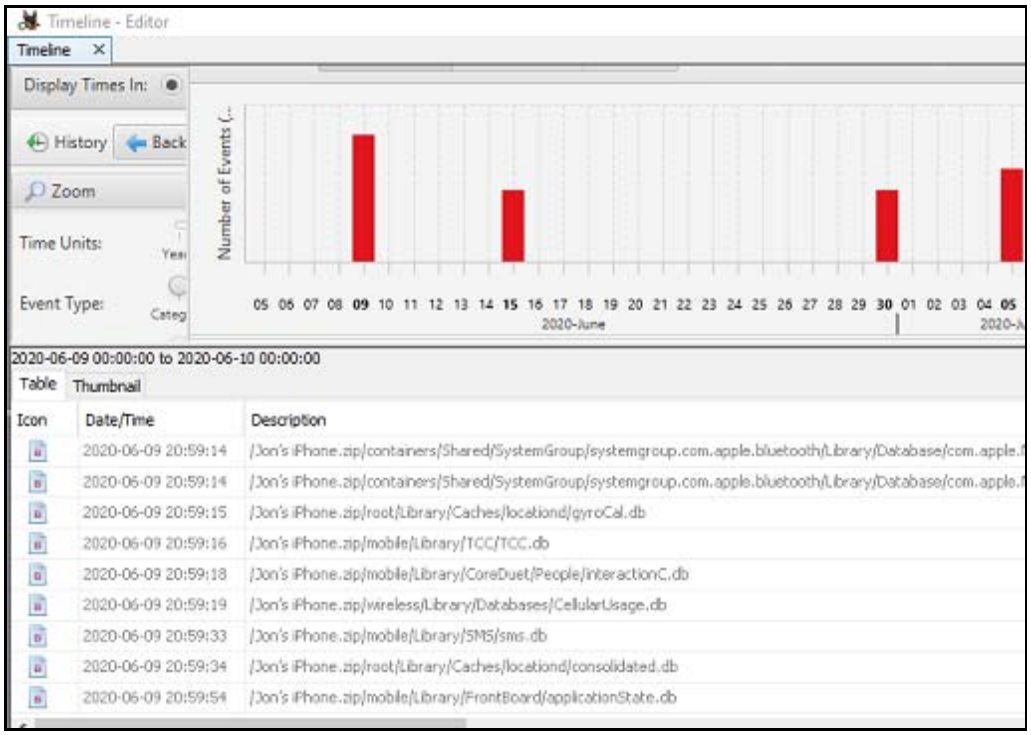


TABLE 1

Question 6

Question 6: What is the model name of this phone (e.g. iPhone 4c)?

Manufacturer's
Expected Response: iPhone 6s

WebCode	Response
232E3H	iPhone 6s
23R6RY	iPhone 6s
2MP2LK	iPhone 6s (iPhone8,1)
2U4K6K	iPhone 6s
2UJ7EL	Apple iPhone 6s
2ZD34D	iPhone 6S
3LXYYV	iPhone 6s
4KQATB	iPhone 6S
4VD9JG	iPhone 6s
6LKHCE	iPhone 6s
6R89XA	Iphone6s
73ULRR	iPhone 6s
7FEZVR	iPhone 6s
7NZ8BH	iPhone 6s
7TZH7H	iPhone 6s
7WXYJC	iPhone 6s
82KA7F	iPhone 6s
8E9BN8	iPhone 6s
8FY44R	iPhone 6s
8XED4T	Apple iPhone 6s
93EEZE	iPhone 6s
9AEVD6	iPhone 6S
9C38CB	iPhone 6s
9J3RE7	iPhone 6s
A8PRHD	iPhone 6s
AB3RE6	iPhone 6s
AJGDN9	iPhone 6s
AUEEZC	iPhone 6s
B7LJQ6	iPhone 6s

TABLE 1

Question 6	
WebCode	**Response**
BGDYWL	iPhone 6s
BK4CEC	iPhone 6s
CMVPWM	iPhone 6s (N71AP)
CTTKD8	iPhone 6s
DDYEJ4	iPhone 6s
DGXQF4	iPhone 6s
DJL3EA	iPhone 6s
EKZT67	iPhone 6s
ET7TE8	iPhone 6s
FNQKQ8	iPhone 6s
FXKMCH	iPhone 6s
G3E42G	Model=iPhone 6s
GA8EUY	iPhone 6s
GJTH2X	iPhone 6s
GXBBQ6	iPhone 6s
HBTH3W	Apple iPhone 6s
HRJN96	iPhone 6s
JRWEYZ	iPhone 6s
KQZJPW	iPhone 6s
L2Z97X	iPhone 6s
L78WJY	iPhone 6s
LDRZQ3	iPhone 6s
LUED6U	iPhone 6s
MK4BJT	iPhone 6s
P94MFP	iPhone 6s
PBRYEU	iPhone 6s
PRFA2W	iPhone 6s
PVHA3U	iPhone 6s
PZYA29	iPhone 6s
Q9J39W	iPhone 6s
QBL2JP	iPhone 6s

TABLE 1

Question 6	
WebCode	**Response**
QTQBNV	iPhone 6s
QZTKUN	iPhone 6S
RA9UVM	iPhone 6s
RWD889	iPhone6s
T6DJYU	iPhone 6s
TGQJVM	iPhone 6s
TL2WDL	iPhone 6s
U2P8ZN	iPhone 6s
UCYFWG	iPhone 6s
UM9CJR	iPhone 6s
UPZBXQ	iPhone 6s
UQBAVK	iPhone 6s
UTYLUQ	iPhone 6s
V6M9DQ	iPhone 6s
VJC6V2	iPhone 6s
VU246Q	iPhone 6s
WJ3TAP	iPhone 6s
WX466N	iPhone 6s
X78WMG	iPhone 6s
X8ZRAP	iPhone 6s
XJGCUL	iPhone 6s
XY9AWG	iPhone 6s
XYELUY	iPhone 6s
YQ9AWF	iPhone 6s
Z8D34E	iPhone 6s
ZB38DY	iPhone 6s
ZX8VNE	iPhone 6S

TABLE 1

Question 6

Question 6: What is the model name of this phone (e.g. iPhone 4c)?

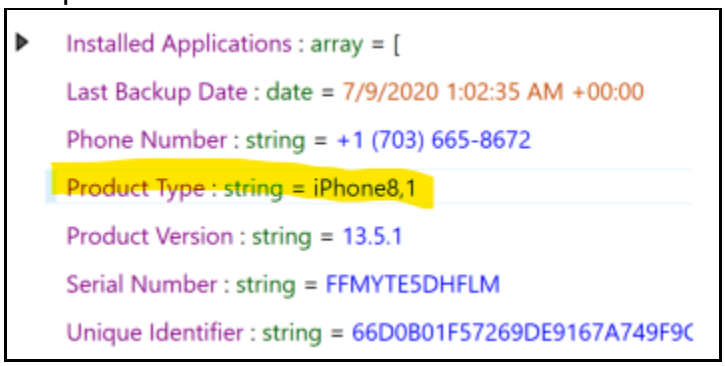
Consensus Result: iPhone 6s

Expected Response Explanation:

This value is parsed from /Backup/Info.plist (stored as Apple mobile device code) by the acquisition tool and stored in the ufd file.

Expected Response Illustration:

Info.plist



AppleDevice_AdvancedLogical.ufd

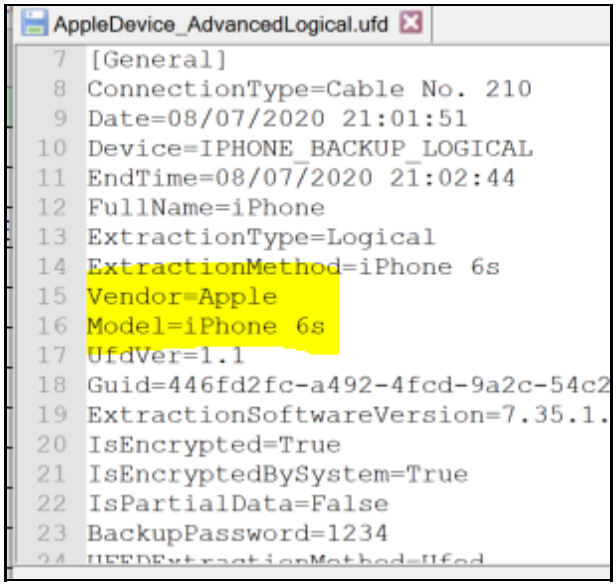


TABLE 1

Question 7

Question 7: What is the version of the operating system on this phone?

Manufacturer's
Expected Response: 13.5.1

WebCode	Response
232E3H	13.5.1
23R6RY	13.5.1
2MP2LK	13.5.1
2U4K6K	13.5.1
2UJ7EL	13.5.1
2ZD34D	13.5.1
3LXYYV	OS 13.5.1
4KQATB	13.5.1
4VD9JG	13.5.1
6LKHCE	13.5.1
6R89XA	13.5.1
73ULRR	13.5.1
7FEZVR	13.5.1
7NZ8BH	13.5.1
7TZH7H	13.5.1
7WXYJC	13.5.1
82KA7F	13.5.1
8E9BN8	13.5.1
8FY44R	13.5.1
8XED4T	13.5.1
93EEZE	13.5.1
9AEVD6	13.5.1
9C38CB	13.5.1
9J3RE7	13.5.1
A8PRHD	13.5.1
AB3RE6	13.5.1
AJGDN9	13.5.1
AUEEZC	13.5.1
B7LJQ6	13.5.1

TABLE 1

Question 7	
WebCode	**Response**
BGDYWL	13.5.1
BK4CEC	13.5.1
CMVPWM	13.5.1
CTTKD8	13.5.1
DDYEJ4	13.5.1
DGXQF4	13.5.1
DJL3EA	13.5.1
EKZT67	13.5.1
ET7TE8	13.5.1
FNQKQ8	13.5.1
FXKMCH	13.5.1
G3E42G	13.5.1
GA8EUY	13.5.1
GJTH2X	13.5.1
GXBBQ6	13.5.1
HBTH3W	13.5.1
HRJN96	13.5.1
JRWEYZ	13.5.1
KQZJPW	13.5.1
L2Z97X	13.5.1
L78WJY	13.5.1
LDRZQ3	13.5.1
LUED6U	13.5.1
MK4BJT	13.5.1
P94MFP	13.5.1
PBRYEU	13.5.1
PRFA2W	13.5.1
PVHA3U	13.5.1
PZYA29	13.5.1
Q9J39W	13.5.1
QBL2JP	13.5.1

TABLE 1

Question 7	
WebCode	**Response**
QTQBNV	13.5.1
QZTKUN	13.5.1
RA9UVM	13.5.1
RWD889	13.5.1
T6DJYU	13.5.1
TGQJVM	13.5.1
TL2WDL	13.5.1
U2P8ZN	13.5.1
UCYFWG	13.5.1
UM9CJR	13.5.1
UPZBXQ	13.5.1
UQBAVK	13.5.1
UTYLUQ	iOS 13.5.1
V6M9DQ	13.5.1
VJC6V2	13.5.1
VU246Q	13.5.1
WJ3TAP	13.5.1
WX466N	13.5.1
X78WMG	13.5.1
X8ZRAP	13.5.1
XJGCUL	13.5.1
XY9AWG	13.5.1
XYELUY	13.5.1
YQ9AWF	13.5.1
Z8D34E	iOS 13.5.1
ZB38DY	13.5.1
ZX8VNE	13.5.1

TABLE 1

Question 7

Question 7: What is the version of the operating system on this phone?

Consensus Result: 13.5.1

Expected Response Explanation:

This information is found in /Lockdown/device_values.plist.

Expected Response Illustration:

device_values.plist

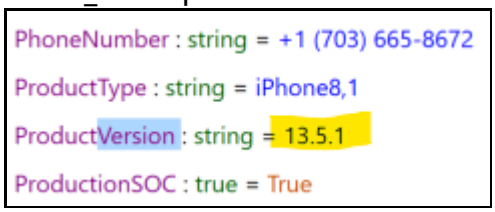


TABLE 1

Question 8

Question 8: What is the set time zone for this phone? Provide answer exactly as shown by the device.

Manufacturer's Expected Response: America/New_York

WebCode	Response
232E3H	America/New_York
23R6RY	(UTC-05:00) New_York (America)
2MP2LK	America/New_York
2U4K6K	(UTC-05:00) New_York (America)
2UJ7EL	(UTC -05:00)New_York (America)
2ZD34D	(UTC-05:00) New_York (America)
3LXYYV	(UTC-05:00) New_York (America)
4KQATB	UTC -05:00 New York (America)
4VD9JG	America/New_York
6LKHCE	(UTC-05:00) New_York (America)
6R89XA	UTC-05:00 New York (america)
73ULRR	(UTC-05:00) New_York (America)
7FEZVR	America/New_York
7NZ8BH	(UTC-05:00) New_York (America)
7TZH7H	America/New_York
7WXYJC	(UTC-05:00) New_York (America)
82KA7F	(UTC-05:00) New_York (America)
8E9BN8	(UTC-05:00) New_York (America)
8FY44R	(UTC-05:00) New_York (America)
8XED4T	(UTC-05:00) New_York (America)
93EEZE	(UTC-05:00) New_York (America)
9AEVD6	(UTC-05:00) New_York (America)
9C38CB	New York
9J3RE7	America/New_York
A8PRHD	America/New_York
AB3RE6	(UTC-0500) New_York (America)
AJGDN9	(UTC -05:00) New_York (America)
AUEEZC	America/New_York
B7LJQ6	(UTC-05:00) New_York (America)

TABLE 1

Question 8	
WebCode	**Response**
BGDYWL	(UTC-05:00) New_York (America)
BK4CEC	(UTC-05:00) New_York (America)
CMVPWM	(UTC-05:00) New_York (America)
CTTKD8	UTC-0500 New_York (America)
DDYEJ4	(UTC-05:00) New_York (America)
DGXQF4	(UTC-05:00) New_York (America)
DJL3EA	(UTC-05:00) New_York (America)
EKZT67	(UTC-05:00) New_York (America)
ET7TE8	(UTC-05:00) New_York (America)
FNQKQ8	(UTC-05:00)New_York (America)
FXKMCH	(UTC-05:00) New_York (America)
G3E42G	(UTC-05:00) New_York (America)
GA8EUY	(UTC-05:00) New_York (America)
GJTH2X	(UTC-05:00) New_York (America)
GXBBQ6	America/New_York
HBTH3W	(UTC-05:00) New_York(America)
HRJN96	(UTC -05:00) New York (America)
JRWEYZ	America/New_York
KQZJPW	(UTC-05:00) New_York (America)
L2Z97X	(UTC-05:00) New_York (America) this is from the Extraction Summary, however, in the device_values.plist file the TimeZone reports as America/New_York
L78WJY	(UTC-05:00) New_York (America)
LDRZQ3	(UTC-05:00) New_York (America)
LUED6U	(UTC-05:00) New_York (America)
MK4BJT	(UTC-05:00) New_York (America)
P94MFP	(UTC-05:00) New_York (America)
PBRYEU	America/New_York
PRFA2W	(UTC -05:00) New_York (America)
PVHA3U	New_York (America)
PZYA29	(UTC-05:00) New_York (America)
Q9J39W	(UTC -05:00) New_York (America)
QBL2JP	UTC-05:00 New York (American)

TABLE 1

Question 8	
WebCode	**Response**
QTQBNV	(UTC-05:00) New_York (America)
QZTKUN	(UTC-05:00) New_York (America)
RA9UVM	(UTC-05:00) New_York (America)
RWD889	(UTC-05:00) New_York (America)
T6DJYU	America/New_York
TGQJVM	(UTC -05:00) New_York (America)
TL2WDL	(UTC-05:00) New_York (America)
U2P8ZN	(UTC-05:00) New_York (America)
UCYFWG	(UTC-05:00) New_York (America)
UM9CJR	America/New York
UPZBXQ	(UTC-05:00) New_York (America)
UQBAVK	(UTC -05:00)New York America
UTYLUQ	(UTC-05:00) New_York (America)
V6M9DQ	(UTC-05:00) New_York (America)
VJC6V2	TimeZone : string = America/New_York
VU246Q	(UTC-05:00) New_York (America)
WJ3TAP	(UTC-05:00) New_York (America)
WX466N	America/New_York
X78WMG	(UTC-05:00) New_York (America)
X8ZRAP	(UTC-05:00) New_York (America)
XJGCUL	America/New_York
XY9AWG	(-05:00) New_York (America)
XYELUY	(UTC-05:00) New York (America)
YQ9AWF	(UTC -05:00) New_York (America)
Z8D34E	America/New_York
ZB38DY	(UTC-05:00) New_York (America)
ZX8VNE	(UTC-05:00) New_York (America)

TABLE 1

Question 8

Question 8: What is the set time zone for this phone? Provide answer exactly as shown by the device.

Consensus Result: America/New_York and all formatting styles which represent the same information.

Expected Response Explanation:
This information is found in /Lockdown/device_values.plist.

Expected Response Illustration:
device_values.plist

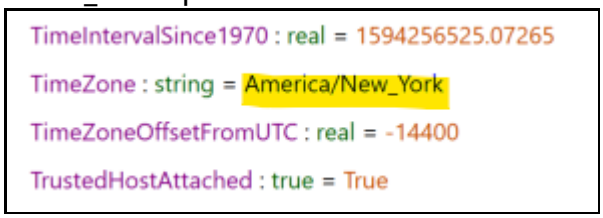


TABLE 1

Question 9

Question 9: What is the ICCID number associated with this phone?

Manufacturer's
Expected Response: 8901260063977237043

WebCode	Response
232E3H	8901260063977237043
23R6RY	8901260063977237043
2MP2LK	8901260063977237043
2U4K6K	8901260063977237043
2UJ7EL	8901260063977237043
2ZD34D	8901260063977237043
3LXYYV	ICCID 8901260063977237043
4KQATB	8901260063977237043
4VD9JG	8901260063977237043
6LKHCE	8901260063977237043
6R89XA	8901260063977237043
73ULRR	8901260063977237043
7FEZVR	8901260063977237043
7NZ8BH	8901260063977237043
7TZH7H	8901260063977237043
7WXYJC	8901260063977237043
82KA7F	8901260063977237043
8E9BN8	8901260063977237043
8FY44R	8901260063977237043
8XED4T	8901260063977237043
93EEZE	8901260063977237043
9AEVD6	8901260063977237043
9C38CB	8901260063977237043
9J3RE7	8901260063977237043
A8PRHD	8901260063977237043
AB3RE6	8901260063977237043
AJGDN9	8901260063977237043
AUEEZC	8901260063977237043
B7LJQ6	8901260063977237043

TABLE 1

Question 9	
WebCode	**Response**
BGDYWL	8901260063977237043
BK4CEC	8901260063977237043
CMVPWM	8901260063977237043
CTTKD8	8901260063977237043
DDYEJ4	8901260063977237043
DGXQF4	8901260063977237043
DJL3EA	8901260063977237043
EKZT67	8901260063977237043
ET7TE8	8901260063977237043
FNQKQ8	8901260063977237043
FXKMCH	8901260063977237043
G3E42G	8901260063977237043
GA8EUY	8901260063977237043
GJTH2X	8901260063977237043
GXBBQ6	8901260063977237043
HBTH3W	8901260063977237043
HRJN96	8901260063977237043
JRWEYZ	8901260063977237043
KQZJPW	8901260063977237043
L2Z97X	8901260063977237043
L78WJY	8901260063977237043
LDRZQ3	8901260063977237043
LUED6U	8901260063977237043
MK4BJT	8901260063977237043
P94MFP	8901260063977237043
PBRYEU	8901260063977237043
PRFA2W	8901260063977237043
PVHA3U	8901260063977237043
PZYA29	8901260063977237043
Q9J39W	8901260063977237043
QBL2JP	8901260063977237043

TABLE 1

Question 9	
WebCode	**Response**
QTQBNV	8901260063977237043
QZTKUN	8901260063977237043
RA9UVM	8901260063977237043
RWD889	8901260063977237043
T6DJYU	8901260063977237043
TGQJVM	8901260063977237043
TL2WDL	8901260063977237043
U2P8ZN	8901260063977237043
UCYFWG	8901260063977237043
UM9CJR	8901260063977237043
UPZBXQ	8901260063977237043
UQBAVK	8901260063977237043
UTYLUQ	8901260063977237043
V6M9DQ	8901260063977237043
VJC6V2	ICCID : string = 8901260063977237043
VU246Q	8901260063977237043
WJ3TAP	8901260063977237043
WX466N	8901260063977237043
X78WMG	8901260063977237043
X8ZRAP	8901260063977237043
XJGCUL	8901260063977237043
XY9AWG	8901260063977237043
XYELUY	8901260063977237043
YQ9AWF	8901260063977237043
Z8D34E	8901260063977237043
ZB38DY	8901260063977237043
ZX8VNE	8901260063977237043

TABLE 1

Question 9

Question 9: What is the ICCID number associated with this phone?

Consensus Result: 8901260063977237043

Expected Response Explanation:

This information is stored in /Backup/Info.plist.

Expected Response Illustration:

Info.plist

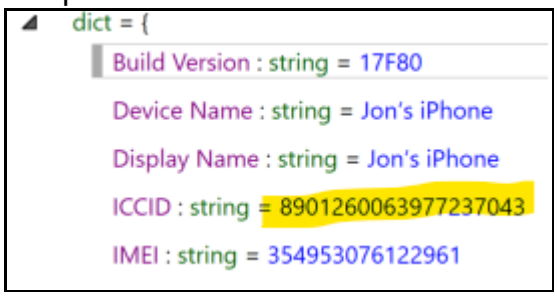


TABLE 1

Question 10

Question 10: Provide the Device Phone Number (MSISDN).

Manufacturer's
Expected Response: 1-703-665-8672

WebCode	Response
232E3H	+1 (703) 665-8672
23R6RY	+17036658672
2MP2LK	1-703-665-8672
2U4K6K	+1 (703) 665-8672
2UJ7EL	+1 (703) 665-8672
2ZD34D	+1 (703) 665-8672
3LXYYV	+1 (703) 665-8672
4KQATB	+1 (703) 6658672
4VD9JG	17036658672
6LKHCE	17036658672
6R89XA	+1 (703) 665-8672
73ULRR	17036658672
7FEZVR	17036658672
7NZ8BH	+1 (703) 665-8672
7TZH7H	+17036658672
7WXYJC	17036658672
82KA7F	+1 (703) 665-8672
8E9BN8	+1 (703) 665-86720 17036658672
8FY44R	+1 (703) 665-8672
8XED4T	+17036658672
93EEZE	+1 (703) 665-8672
9AEVD6	+17036658672
9C38CB	+17036658672
9J3RE7	+1 (703) 665-8672
A8PRHD	17036658672
AB3RE6	+1 (703) 665-8672
AJGDN9	+ 1 (703) 665-8672
AUEEZC	+1 (703) 665-8672
B7LJQ6	17036658672

TABLE 1

Question 10	
WebCode	**Response**
BGDYWL	+1 (703) 665-8672
BK4CEC	+17036658672
CMVPWM	+1 (703) 665-8672
CTTKD8	+1 (703) 665-8672
DDYEJ4	17036658672
DGXQF4	17036658672
DJL3EA	17036658672
EKZT67	17036658672
ET7TE8	17036658672
FNQKQ8	+17036658672
FXKMCH	+1(703)665-8672
G3E42G	+1 (703) 665-8672
GA8EUY	+1 (703) 665-8672
GJTH2X	1 (703) 665-8672
GXBBQ6	17036658672
HBTH3W	+1 (703) 665-8672
HRJN96	+17036658672
JRWEYZ	17036658672
KQZJPW	703-665-8672 (MSISDN: 17036658672)
L2Z97X	1 (703) 665-8672
L78WJY	+1(703)-665-8672
LDRZQ3	+1 (703) 665-8672
LUED6U	1 (703) 665-8672
MK4BJT	17036658672
P94MFP	+1 (703) 665-8672
PBRYEU	+1 (703) 665-8672
PRFA2W	+1(703)665-8672
PVHA3U	+1 (703)665-8672
PZYA29	7036658672
Q9J39W	17036658672
QBL2JP	+1(703)655-8672

TABLE 1

Question 10	
WebCode	**Response**
QTQBNV	+1 (703) 665-8672
QZTKUN	703-665-8672
RA9UVM	+17036658672
RWD889	+1(703)665-8672
T6DJYU	17036658672
TGQJVM	17036658672
TL2WDL	17036658672
U2P8ZN	17036658672 or +1 (703) 665-8672
UCYFWG	+1 (703) 665-8672
UM9CJR	+1 (703) 665-8672
UPZBXQ	+1 (703) 665-8672
UQBAVK	+1 (703) 665-8672
UTYLUQ	+1 (703) 665-8672
V6M9DQ	17036658672
VJC6V2	+17036658672
VU246Q	17036658672
WJ3TAP	+1 (703) 665-8672
WX466N	+1 (703) 665-8672
X78WMG	+1 (703) 665-8672
X8ZRAP	+1(703) 665-8672
XJGCUL	+17036658672
XY9AWG	1-703-665-8672
XYELUY	17036658672
YQ9AWF	+1(703)665-8672
Z8D34E	17036658672
ZB38DY	+1 (703) 665-8672
ZX8VNE	+17036658672en-US

TABLE 1

Question 10

Question 10: Provide the Device Phone Number (MSISDN).

Consensus Result: 1-703-665-8672

Expected Response Explanation:

This information is stored in /Backup/Info.plist.

Expected Response Illustration:

Info.plist

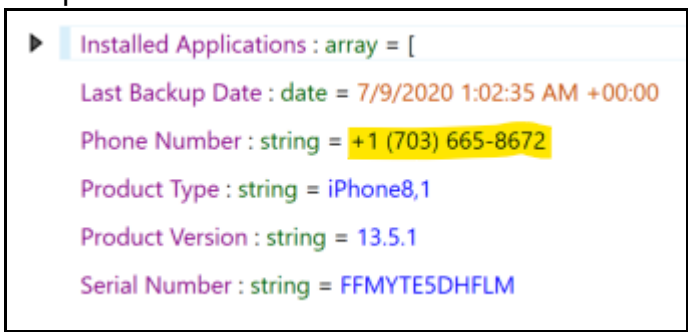


TABLE 1

Question 11

Question 11: What is the language setting for this phone?

Manufacturer's
Expected Response: en-US

WebCode	Response
232E3H	en-US (US English)
23R6RY	En_US
2MP2LK	en_US (English)
2U4K6K	en_US
2UJ7EL	en_US
2ZD34D	en_US
3LXYYV	en_US
4KQATB	en-US
4VD9JG	en-US
6LKHCE	English (United States)
6R89XA	en_US
73ULRR	en_US
7FEZVR	en_US
7NZ8BH	en_US
7TZH7H	en-US
7WXYJC	en_US
82KA7F	en_US
8E9BN8	en_US
8FY44R	en_US
8XED4T	en_US
93EEZE	en_US
9AEVD6	en_US
9C38CB	en_US
9J3RE7	en_US
A8PRHD	en_US
AB3RE6	en_US
AJGDN9	en_us
AUEEZC	en-US
B7LJQ6	en_US

TABLE 1

Question 11	
WebCode	**Response**
BGDYWL	en_US
BK4CEC	en_US
CMVPWM	en_US
CTTKD8	en_US
DDYEJ4	en_US
DGXQF4	en_US
DJL3EA	en_US (English)
EKZT67	en_US
ET7TE8	en_US
FNQKQ8	en_US
FXKMCH	en_US
G3E42G	en_US
GA8EUY	en_US
GJTH2X	en_US
GXBBQ6	en-US
HBTH3W	en_US
HRJN96	en_US
JRWEYZ	en_US
KQZJPW	en_US (English)
L2Z97X	en_US
L78WJY	en_us
LDRZQ3	en_US
LUED6U	en_US; English
MK4BJT	en_US
P94MFP	en_US
PBRYEU	en_US
PRFA2W	en_US
PVHA3U	en_US
PZYA29	en_US
Q9J39W	en_US
QBL2JP	English. en_US

TABLE 1

Question 11	
WebCode	**Response**
QTQBNV	en_US
QZTKUN	English
RA9UVM	en_US
RWD889	en_US
T6DJYU	en-US
TGQJVM	en_US
TL2WDL	En_US
U2P8ZN	en_US
UCYFWG	en_US
UM9CJR	en_US
UPZBXQ	en_US
UQBAVK	English US
UTYLUQ	en_US (English-United States)
V6M9DQ	en_US
VJC6V2	Language : string = en-US (English)
VU246Q	en_US
WJ3TAP	en_US
WX466N	en-US
X78WMG	en_US
X8ZRAP	en_US English
XJGCUL	en-US
XY9AWG	en_US English
XYELUY	English
YQ9AWF	en_US
Z8D34E	en_US
ZB38DY	en_US
ZX8VNE	en-US

TABLE 1

Question 11

Question 11: What is the language setting for this phone?

Consensus Result: en-US and all formatting styles which represent the same information.

Expected Response Explanation:

This information is stored in /Lockdown/device_values.plist.

Expected Response Illustration:

device_values.plist

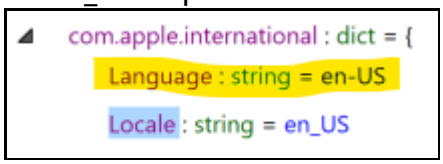


TABLE 1

Question 12

Question 12: Was icloud backup enabled? Provide a Yes/No response.

Manufacturer's Expected Response: No

WebCode	Response
232E3H	No
23R6RY	No
2MP2LK	No
2U4K6K	No
2UJ7EL	No
2ZD34D	No
3LXYYV	no
4KQATB	No
4VD9JG	No
6LKHCE	No
6R89XA	No.
73ULRR	No
7FEZVR	No
7NZ8BH	No
7TZH7H	No
7WXYJC	No
82KA7F	no
8E9BN8	No
8FY44R	No
8XED4T	No
93EEZE	No
9AEVD6	No
9C38CB	No
9J3RE7	No
A8PRHD	No
AB3RE6	Yes
AJGDN9	No
AUEEZC	No
B7LJQ6	No

TABLE 1

Question 12	
WebCode	**Response**
BGDYWL	No
BK4CEC	No
CMVPWM	No
CTTKD8	No
DDYEJ4	No
DGXQF4	No
DJL3EA	No
EKZT67	No
ET7TE8	No
FNQKQ8	No
FXKMCH	No
G3E42G	No
GA8EUY	No/False
GJTH2X	No.
GXBBQ6	No
HBTH3W	No
HRJN96	False
JRWEYZ	No
KQZJPW	No
L2Z97X	No
L78WJY	NO
LDRZQ3	No
LUED6U	No
MK4BJT	No
P94MFP	False
PBRYEU	No
PRFA2W	No
PVHA3U	No
PZYA29	No
Q9J39W	No (False)
QBL2JP	No

TABLE 1

Question 12	
WebCode	**Response**
QTQBNV	No
QZTKUN	No
RA9UVM	No
RWD889	No
T6DJYU	No
TGQJVM	No
TL2WDL	No
U2P8ZN	No
UCYFWG	No
UM9CJR	No
UPZBXQ	No
UQBAVK	No
UTYLUQ	No
V6M9DQ	No
VJC6V2	No
VU246Q	False
WJ3TAP	No
WX466N	No
X78WMG	No
X8ZRAP	No
XJGCUL	No
XY9AWG	No
XYELUY	No
YQ9AWF	No
Z8D34E	No
ZB38DY	No
ZX8VNE	NO

TABLE 1

Question 12

Question 12: Was icloud backup enabled? Provide a Yes/No response.

Consensus Result: No (False)

Expected Response Explanation:

This information is stored in /Lockdown/device_values.plist.

Expected Response Illustration:

device_values.plist

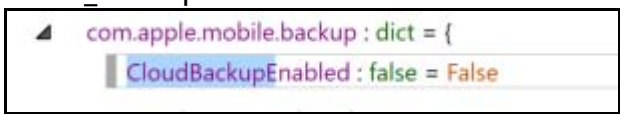


TABLE 1

Question 13

Question 13: Provide the AppleID associated with this phone.

Manufacturer's Expected Response: jon.daniels39@icloud.com

WebCode	Response
232E3H	jon.daniels39@icloud.com
23R6RY	jon.daniels39@icloud.com
2MP2LK	jon.daniels39@icloud.com
2U4K6K	jon.daniels39@icloud.com
2UJ7EL	jon.daniels39@icloud.com
2ZD34D	jon.daniels39@icloud.com
3LXYYV	jon.daniels39@icloud.com
4KQATB	jon.daniels39@icloud.com
4VD9JG	jon.daniels39@icloud.com
6LKHCE	jon.daniels39@icloud.com
6R89XA	jon.daniels39@icloud.com
73ULRR	jon.daniels39@icloud.com
7FEZVR	jon.daniels39@icloud.com
7NZ8BH	jon.daniels39@icloud.com
7TZH7H	jon.daniels39@icloud.com
7WXYJC	jon.daniels39@icloud.com
82KA7F	jon.daniels39@icloud.com
8E9BN8	jon.daniels39@icloud.com
8FY44R	jon.daniels39@icloud.com
8XED4T	jon.daniels39@icloud.com
93EEZE	jon.daniels39@icloud.com
9AEVD6	jon.daniels39@icloud.com
9C38CB	jon.daniels39@icloud.com
9J3RE7	jon.daniels39@icloud.com
A8PRHD	jon.daniels39@icloud.com
AB3RE6	jon.daniels39@icloud.com
AJGDN9	jon.daniels39@icloud.com
AUEEZC	jon.daniels39@icloud.com
B7LJQ6	jon.daniels39@icloud.com

TABLE 1

Question 13	
WebCode	**Response**
BGDYWL	jon.daniels39@icloud.com
BK4CEC	jon.daniels39@icloud.com
CMVPWM	jon.daniels39@icloud.com
CTTKD8	jon.daniels39@icloud.com
DDYEJ4	jon.daniels39@icloud.com
DGXQF4	jon.daniels39@icloud.com
DJL3EA	jon.daniels39@icloud.com
EKZT67	jon.daniels39@icloud.com
ET7TE8	jon.daniels39@icloud.com
FNQKQ8	jon.daniels39@icloud.com
FXKMCH	jon.daniels39@icloud.com
G3E42G	jon.daniels39@icloud.com
GA8EUY	jon.daniels39@icloud.com
GJTH2X	jon.daniels39@icloud.com
GXBBQ6	jon.daniels39@icloud.com
HBTH3W	jon.daniels39@icloud.com
HRJN96	jon.daniels39@icloud.com
JRWEYZ	jon.daniels39@icloud.com
KQZJPW	jon.daniels39@icloud.com
L2Z97X	jon.daniels39@icloud.com
L78WJY	jon.daniels39@icloud.com
LDRZQ3	jon.daniels39@icloud.com
LUED6U	jon.daniels39@icloud.com
MK4BJT	jon.daniels39@icloud.com
P94MFP	jon.daniels39@icloud.com
PBRYEU	jon.daniels39@icloud.com
PRFA2W	jon.daniels39@icloud.com
PVHA3U	jon.daniels39@icloud.com
PZYA29	jon.daniels39@icloud.com
Q9J39W	jon.daniels39@icloud.com
QBL2JP	jon.daniels39@icloud.com

TABLE 1

Question 13	
WebCode	**Response**
QTQBNV	jon.daniels39@icloud.com
QZTKUN	jon.daniels39@icloud.com
RA9UVM	jon.daniels39@icloud.com
RWD889	jon.daniels39@icloud.com
T6DJYU	jon.daniels39@icloud.com
TGQJVM	jon.daniels39@icloud.com
TL2WDL	jon.daniels39@icloud.com
U2P8ZN	jon.daniels39@icloud.com
UCYFWG	jon.daniels39@icloud.com
UM9CJR	jon.daniels39@icloud.com
UPZBXQ	jon.daniels39@icloud.com
UQBAVK	jon.daniels39@icloud.com
UTYLUQ	jon.daniels39@icloud.com
V6M9DQ	jon.daniels39@icloud.com
VJC6V2	jon.daniels39@icloud.com
VU246Q	jon.daniels39@icloud.com
WJ3TAP	jon.daniels39@icloud.com
WX466N	jon.daniels39@icloud.com
X78WMG	jon.daniels39@icloud.com
X8ZRAP	jon.daniels39@icloud.com
XJGCUL	jon.daniels39@icloud.com
XY9AWG	Jon.daniels39@icloud.com
XYELUY	jon.daniels39@icloud.com
YQ9AWF	jon.daniels39@icloud.com
Z8D34E	jon.daniels39@icloud.com
ZB38DY	jon.daniels39@icloud.com
ZX8VNE	jon.daniels39@icloud.com

TABLE 1

Question 13

Question 13: Provide the AppleID associated with this phone.

Consensus Result: jon.daniels39@icloud.com

Expected Response Explanation:

This information is stored in /mobile/Library/Accounts/Accounts3.sqlite.

Expected Response Illustration:

Accounts3.sqlite

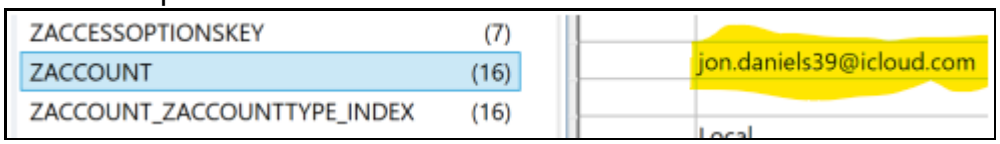


TABLE 1

Question 14

Question 14: What is the SSID (name) of the LAST WiFi Hotspot connected to this phone?

Manufacturer's
Expected Response: MBR-f4b

WebCode	Response
232E3H	MBR-f4b
23R6RY	MBR-f4b
2MP2LK	MBR-f4b
2U4K6K	MBR-f4b
2UJ7EL	MBR-f4b
2ZD34D	MBR-f4b
3LXYYV	MBR-f4b
4KQATB	MBR-f4b
4VD9JG	MBR-f4b
6LKHCE	MBR-f4b
6R89XA	hotspot123
73ULRR	MBR-f4b
7FEZVR	MBR-f4b
7NZ8BH	MBR-f4b
7TZH7H	MBR-f4b
7WXYJC	MBR-f4b
82KA7F	MBR-f4b
8E9BN8	MBR-f4b
8FY44R	MBR-f4b
8XED4T	MBR-f4b
93EEZE	MBR-f4b
9AEVD6	MBR-f4b
9C38CB	MBR-f4b
9J3RE7	hotspot123
A8PRHD	MBR-f4b
AB3RE6	MBR-f4b
AJGDN9	MBR-F4b
AUEEZC	MBR-f4b
B7LJQ6	MBR-f4b

TABLE 1

Question 14	
WebCode	**Response**
BGDYWL	MBR-f4b
BK4CEC	MBR-f4b
CMVPWM	MBR-f4b
CTTKD8	MBR-f4b
DDYEJ4	MBR-f4b
DGXQF4	MBR-f4b
DJL3EA	MBR-f4b
EKZT67	MBR-f4b
ET7TE8	MBR-f4b
FNQKQ8	MBR-f4b
FXKMCH	MBR-f4b
G3E42G	MBR-f4b
GA8EUY	MBR-f4b
GJTH2X	hotspot123
GXBBQ6	MBR-f4b
HBTH3W	MBR-f4b
HRJN96	MBR-f4b
JRWEYZ	MBR-f4b
KQZJPW	MBR-f4b
L2Z97X	MBR-f4b
L78WJY	MBR-f4b
LDRZQ3	MBR-f4b
LUED6U	MBR-f4b
MK4BJT	MBR-f4b
P94MFP	MBR-f4b
PBRYEU	MBR-f4b
PRFA2W	MBR-f4b
PVHA3U	MBR-f4b
PZYA29	MBR-f4b
Q9J39W	MBR-f4b
QBL2JP	RCMP Surveillance Moose

TABLE 1

Question 14	
WebCode	**Response**
QTQBNV	MBR-f4b
QZTKUN	MBR-f4b
RA9UVM	MBR-f4b
RWD889	MBR-f4b
T6DJYU	MBR-f4b
TGQJVM	MBR-f4b
TL2WDL	Hotspot123
U2P8ZN	MBR-f4b
UCYFWG	hotspot123
UM9CJR	MBR-f4b
UPZBXQ	MBR-f4b
UQBAVK	hotspot123
UTYLUQ	MBR-f4b
V6M9DQ	MBR-f4b
VJC6V2	MBR-f4b
VU246Q	MBR-f4b
WJ3TAP	MBR-f4b
WX466N	MBR-f4b
X78WMG	MBR-f4b
X8ZRAP	MBR-fab
XJGCUL	MBR-f4b
XY9AWG	Hotspot123
XYELUY	MBR-f4b
YQ9AWF	MBR-f4b
Z8D34E	MBR-f4b
ZB38DY	MBR-f4b
ZX8VNE	MBR-f4b

TABLE 1

Question 14

Question 14: What is the SSID (name) of the LAST WiFi Hotspot connected to this phone?

Consensus Result: MBR-f4b

Expected Response Explanation:

This information is stored in /preferences/SystemConfiguration/com.apple.wifi.plist.

Expected Response Illustration:

com.apple.wifi.plist

Cellebrite "Wireless Networks" table parsed from com.apple.wifi.plist

Timestamp	End time	BSSID	SSId
		0:30:44:4:2f:4b	MBR-f4b
		5e:36:d4:29:cb:2e	RCMP Surveillance Moose
			Apple Store
6/28/2020 11:38:31 AM(UTC-4)			hotspot123
6/28/2020 1:27:42 PM(UTC-4)		6A:67:FD:75:65:99	hotspot123
6/28/2020 12:52:33 PM(UTC-4)		0A:6C:6C:5E:B6:02	hotspot123
6/28/2020 12:03:09 PM(UTC-4)		16:E7:86:C9:A9:AA	hotspot123
6/28/2020 11:38:31 AM(UTC-4)		1A:8B:AA:B1:45:8C	hotspot123
6/27/2020 1:09:05 PM(UTC-4)		5e:36:d4:29:cb:2e	RCMP Surveillance Moose
7/6/2020 7:49:58 AM(UTC-4)		0:30:44:4:2f:4b	MBR-f4b

Other Responses:

Six participants reported Hotspot123 which is a WiFi hotspot but not the last one connected to this phone.

TABLE 1

Question 15

Question 15: Provide the BSSID of the WiFi Hotspot connected to this phone on 6/28/2020 at 12:52:33 PM (UTC-4)?

Manufacturer's Expected Response: 0A:6C:6C:5E:B6:02

WebCode	Response
232E3H	0a:6c:6c:5e:b6:02
23R6RY	0A:6C:6C:5E:B6:02
2MP2LK	0A:6C:6C:5E:B6:02
2U4K6K	0A:6C:6C:5E:B6:02
2UJ7EL	0A:6C:6C:5E:B6:02
2ZD34D	hotspot123
3LXYYV	0A:6C:6C:5E:B6:02
4KQATB	0A:6C:6C:5E:B6:02
4VD9JG	0A:6C:6C:5E:B6:02
6LKHCE	0A:6C:6C:5E:B6:02
6R89XA	0A:6C:6C:5E:B6:02
73ULRR	0A:6C:6C:5E:B6:02
7FEZVR	0A:6C:6C:5E:B6:02
7NZ8BH	0A:6C:6C:5E:B6:02
7TZH7H	0A:6C:6C:5E:B6:02
7WXYJC	0A:6C:6C:5E:B6:02
82KA7F	0A:6C:6C:5E:B6:02
8E9BN8	0A:6C:6C:5E:B6:02
8FY44R	0A:6C:6C:5E:B6:02
8XED4T	0A:6C:6C:5E:B6:02
93EEZE	0A:6C:6C:5E:B6:02
9AEVD6	0A:6C:6C:5E:B6:02
9C38CB	0A:6C:6C:5E:B6:02
9J3RE7	0A:6C:6C:5E:B6:02
A8PRHD	0A:6C:6C:5E:B6:02
AB3RE6	0A:6C:6C:5E:B6:02
AJGDN9	0A:6C:6C:5E:B6:02
AUEEZC	0A:6C:6C:5E:B6:02

TABLE 1

Question 15	
WebCode	**Response**
B7LJQ6	0A:6C:6C:5E:B6:02
BGDYWL	0A:6C:6C:5E:B6:02
BK4CEC	0A:6C:6C:5E:B6:02
CMVPWM	0A:6C:6C:5E:B6:02
CTTKD8	hotspot123
DDYEJ4	0A:6C:6C:5E:B6:02
DGXQF4	0A:6C:6C:5E:B6:02
DJL3EA	0A:6C:6C:5E:B6:02
EKZT67	0A:6C:6C:5E:B6:02
ET7TE8	0A:6C:6C:5E:B6:02
FNQKQ8	0A:6C:6C:5E:B6:02
FXKMCH	0A:6C:6C:5E:B6:02
G3E42G	0A:6C:6C:5E:B6:02
GA8EUY	0A:6C:6C:5E:B6:02
GJTH2X	0A:6C:6C:5E:B6:02
GXBBQ6	0A:6C:6C:5E:B6:02
HBTH3W	0A:6C:6C:5E:B6:02
HRJN96	hotspot123
JRWEYZ	0A:6C:6C:5E:B6:02
KQZJPW	hotspot123
L2Z97X	0A:6C:6C:5E:B6:02
L78WJY	0A:6C:6C:5E:B6:02
LDRZQ3	0A:6C:6C:5E:B6:02
LUED6U	0A:6C:6C:5E:B6:02
MK4BJT	0A:6C:6C:5E:B6:02
P94MFP	0A:6C:6C:5E:B6:02
PBRYEU	0A:6C:6C:5E:B6:02
PRFA2W	0A:6C:6C:5E:B6:02
PVHA3U	0A:6C:6C:5E:B6:02
PZYA29	0A:6C:6C:5E:B6:02
Q9J39W	0A:6C:6C:5E:B6:02

TABLE 1

Question 15	
WebCode	**Response**
QBL2JP	0A:6C:6C:5E:B6:02
QTQBNV	0A:6C:6C:5E:B6:02
QZTKUN	0A:6C:6C:5E:B6:02
RA9UVM	0A:6C:6C:5E:B6:02
RWD889	0A:6C:6C:5E:B6:02
T6DJYU	0A:6C:6C:5E:B6:02
TGQJVM	OA:6C:6C:5E:B6:02
TL2WDL	0A:6C:6C:5E:B6:02
U2P8ZN	0A:6C:6C:5E:B6:02
UCYFWG	0A:6C:6C:5E:B6:02
UM9CJR	0A:6C:6C:5E:B6:02
UPZBXQ	0A:6C:6C:5E:B6:02
UQBAVK	0A:6C:6C:5E:B6:02
UTYLUQ	0A:6C:6C:5E:B6:02
V6M9DQ	0A:6C:6C:5E:B6:02
VJC6V2	0A:6C:6C:5E:B6:02
VU246Q	0A:6C:6C:5E:B6:02
WJ3TAP	0A:6C:6C:5E:B6:02
WX466N	0A:6C:6C:5E:B6:02
X78WMG	0A:6C:6C:5E:B6:02
X8ZRAP	0A:6C:6C:5E:b6:02
XJGCUL	0A:6C:6C:5E:B6:02
XY9AWG	0A:6C:6C:5E:B6:02
XYELUY	0A:6C:6C:5E:B6:02
YQ9AWF	0A:6C:6C:5E:B6:02
Z8D34E	0A:6C:6C:5E:B6:02
ZB38DY	0A:6C:6C:5E:B6:02
ZX8VNE	0A:6C:6C:5E:B6:02

TABLE 1

Question 15

Question 15: Provide the BSSID of the WiFi Hotspot connected to this phone on 6/28/2020 at 12:52:33 PM (UTC-4)?

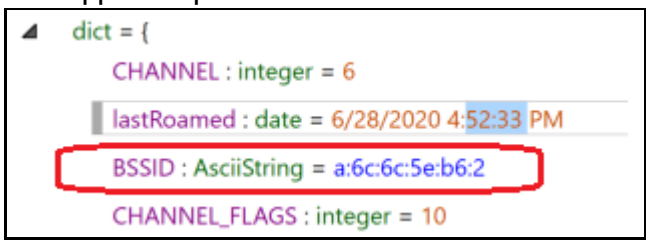
Consensus Result: 0A:6C:6C:5E:B6:02. Any slight variation of the expected result was disregarded as an outlier if it was easily determined to be a typographical error.

Expected Response Explanation:

This information is stored in /preferences/SystemConfiguration/com.apple.wifi.plist.

Expected Response Illustration:

com.apple.wifi.plist



Cellebrite "Wireless Networks" table parsed from com.apple.wifi.plist

Wireless Networks (10)

Graphical timebar

Timestamp	End time	BSSID	SSId
7/6/2020 7:49:58 AM(UTC-4)		0:30:44:4:2f:4b	MBR-f4b
6/28/2020 1:27:42 PM(UTC-4)		6A:67:FD:75:65:99	hotspot123
6/28/2020 12:52:33 PM(UTC-4)		0A:6C:6C:5E:B6:02	hotspot123
6/28/2020 12:03:09 PM(UTC-4)		16:E7:86:C9:A9:AA	hotspot123
6/28/2020 11:38:31 AM(UTC-4)		1A:8B:AA:B1:45:8C	hotspot123
6/28/2020 11:38:31 AM(UTC-4)			hotspot123
6/27/2020 1:09:05 PM(UTC-4)		5e:36:d4:29:cb:2e	RCMP Surveillance Moose
			Apple Store
		5e:36:d4:29:cb:2e	RCMP Surveillance Moose
		0:30:44:4:2f:4b	MBR-f4b

TABLE 1

Question 16

Question 16: What is the make and model of the device with MAC Address 00:6A:8E:02:E9:2E?

Manufacturer's
Expected Response: TaoTronics TT-BH041

WebCode	Response
232E3H	TaoTronics TT-BH041
23R6RY	TaoTronics TT-BH041
2MP2LK	TaoTronics TT-BH041
2U4K6K	TaoTronics TT-BH041
2UJ7EL	TaoTronics TT-BH041
2ZD34D	TaoTronics TT-BH041
3LXYYV	TaoTronics TT-BH041
4KQATB	TaoTronics TT-BH041
4VD9JG	TaoTronics TT-BH041
6LKHCE	Make: TaoTronics Model: TT-BH041
6R89XA	TaoTronics TT-BH041
73ULRR	TaoTronics TT-BH041
7FEZVR	TaoTronics TT-BH041
7NZ8BH	TaoTronics TT-BH041
7TZH7H	TaoTronics TT-BH041
7WXYJC	TaoTronics TT-BH041
82KA7F	Device type: Headset, device name: TaoTronics TT-BH041
8E9BN8	TaoTronics TT-BH041
8FY44R	TaoTronics TT-BH041
8XED4T	TaoTronics TT-BH041
93EEZE	TaoTronics TT-BH041
9AEVD6	TaoTronics TT-BH041
9C38CB	TaoTronics TT-BH041
9J3RE7	TaoTronics TT-BH041
A8PRHD	TaoTronics TT-BH041
AB3RE6	TaoTronics TT-BH041
AJGDN9	TaoTronics TT-BH041
AUEEZC	TaoTronics TT-BH041
B7LJQ6	TaoTronics TT-BH041

TABLE 1

Question 16	
WebCode	**Response**
BGDYWL	TaoTronics TT-BH041
BK4CEC	TaoTronics TT-BH041
CMVPWM	TaoTronics TT-BH041
CTTKD8	TaoTronics TT-BH041
DDYEJ4	TaoTronics TT-BH041
DGXQF4	TaoTronics TT-BH041
DJL3EA	TaoTronics TT-BH041
EKZT67	TaoTronics TT-BH041
ET7TE8	TaoTronics TT-BH041
FNQKQ8	TaoTronics TT-BH041
FXKMCH	TaoTronics TT-BH041
G3E42G	TaoTronics TT-BH041
GA8EUY	TaoTronics TT-BH041
GJTH2X	TaoTronics TT-BH041
GXBBQ6	TaoTronics TT-BH041
HBTH3W	TaoTronics TT-BH041(headset)
HRJN96	TaoTronics TT-BH041
JRWEYZ	TaoTronics TT-BH041
KQZJPW	TaoTronics TT-BH041
L2Z97X	TaoTronics TT-BH041
L78WJY	TaoTronics TT-BH041
LDRZQ3	TaoTronics TT-BH041
LUED6U	TaoTronics, TT-BH041
MK4BJT	TaoTronics TT-BH041
P94MFP	TaoTronics TT-BH041
PBRYEU	TaoTronics TT-BH041
PRFA2W	TaoTronics TT-BH041
PVHA3U	TaoTronics TT-BH041
PZYA29	TaoTronics TT-BH041
Q9J39W	TaoTronics TT-BH041
QBL2JP	TaoTronics TT-BH041

TABLE 1

Question 16	
WebCode	**Response**
QTQBNV	TaoTronics TT-BH041
QZTKUN	TaoTronics TT-BH041 headset
RA9UVM	TaoTronics TT-BH041 headphones
RWD889	TaoTronics TT-BH041
T6DJYU	TaoTronics TT-BH041
TGQJVM	Tao Tronics TT-BH041
TL2WDL	TaoTronics TT-BH041
U2P8ZN	TaoTronics TT-BH041
UCYFWG	TaoTronics TT-BH041
UM9CJR	TaoTronics TT-BH041
UPZBXQ	TaoTronics TT-BH041
UQBAVK	TaoTronics TT-BH041
UTYLUQ	Make: TaoTronics Model: TT-BH041
V6M9DQ	TaoTronics TT-BH041
VJC6V2	TaoTronics TT-BH041
VU246Q	TaoTronics TT-BH041
WJ3TAP	TaoTronics TT-BH041
WX466N	TaoTronics TT-BH041
X78WMG	TaoTronics TT-BH041
X8ZRAP	Tao Tronics TT-BH041
XJGCUL	TaoTronics TT-BH041
XY9AWG	TaoTronics TT-BH041
XYELUY	TaoTronics TT-BH041
YQ9AWF	TaoTronics TT-BH041
Z8D34E	TaoTronics TT-BH041
ZB38DY	TaoTronics TT-BH041
ZX8VNE	TaoTronics TT-BH041

TABLE 1

Question 16

Question 16: What is the make and model of the device with MAC Address 00:6A:8E:02:E9:2E?

Consensus Result: TaoTronics TT-BH041

Expected Response Explanation:

This information is stored in /containers/Shared/SystemGroup/systemgroup.com.apple.bluetooth/Library/Preferences/com.apple.MobileBluetooth.devices.plist.

Expected Response Illustration:

com.apple.MobileBluetooth.devices.plist

Cellebrite "Bluetooth" table parsed from com.apple.MobileBluetooth.devices.plist

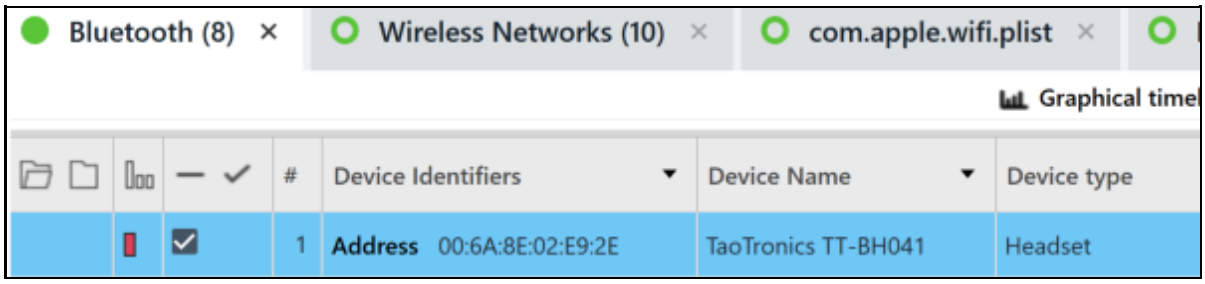


TABLE 1

Question 17

Question 17: What is the name of the user-installed (i.e. non-Apple) email app?

Manufacturer's Expected Response: ProtonMail

WebCode	Response
232E3H	ProtonMail
23R6RY	ProtonMail
2MP2LK	ProtonMail
2U4K6K	ProtonMail
2UJ7EL	ProtonMail
2ZD34D	ProtonMai
3LXYYV	ProtonMail
4KQATB	ProtonMail
4VD9JG	ProtonMail
6LKHCE	ProtonMail
6R89XA	ProtonMail
73ULRR	ProtonMail
7FEZVR	ProtonMail
7NZ8BH	ProtonMail
7TZH7H	ProtonMail
7WXYJC	ProtonMail
82KA7F	ProtonMail
8E9BN8	ProtonMail
8FY44R	ProtonMail
8XED4T	ProtonMail
93EEZE	ProtonMail
9AEVD6	ProtonMail
9C38CB	ProtonMail
9J3RE7	ProtonMail
A8PRHD	ProtonMail
AB3RE6	ProtonMail
AJGDN9	ProtonMail
AUEEZC	ProtonMail
B7LJQ6	Proton Mail

TABLE 1

Question 17	
WebCode	**Response**
BGDYWL	ProtonMail
BK4CEC	Protonmail
CMVPWM	ProtonMail
CTTKD8	ProtonMail
DDYEJ4	ProtonMail
DGXQF4	ProtonMail
DJL3EA	ProtonMail
EKZT67	ProtonMail
ET7TE8	ProtonMail
FNQKQ8	ProtonMail
FXKMCH	ProtonMail
G3E42G	ProtonMail
GA8EUY	ProtonMail
GJTH2X	ProtonMail
GXBBQ6	ProtonMail
HBTH3W	ProtonMail
HRJN96	ProtonMail
JRWEYZ	ProtonMail
KQZJPW	ProtonMail
L2Z97X	ProtonMail
L78WJY	ProtonMail
LDRZQ3	ProtonMail
LUED6U	ProtonMail
MK4BJT	ProtonMail
P94MFP	ProtonMail
PBRYEU	ProtonMail
PRFA2W	ProtonMail
PVHA3U	ProtonMail
PZYA29	ProtonMail
Q9J39W	ProtonMail
QBL2JP	MobileMail

TABLE 1

Question 17	
WebCode	**Response**
QTQBNV	ProtonMail
QZTKUN	ProtonMail
RA9UVM	ProtonMail
RWD889	ProtonMail
T6DJYU	ProtonMail
TGQJVM	ProtonMail
TL2WDL	ProtonMail
U2P8ZN	ProtonMail
UCYFWG	ProtonMail
UM9CJR	ProtonMail
UPZBXQ	ProtonMail
UQBAVK	ProtonMail
UTYLUQ	Proton Mail
V6M9DQ	ProtonMail
VJC6V2	Proton Mail
VU246Q	ProtonMail
WJ3TAP	ProtonMail
WX466N	ProtonMail
X78WMG	ProtonMail
X8ZRAP	Proton Mail
XJGCUL	ProtonMail
XY9AWG	Protonmail
XYELUY	ProtonMail
YQ9AWF	Protonmail
Z8D34E	ProtonMail
ZB38DY	ProtonMail
ZX8VNE	Proton Mail

TABLE 1

Question 17

Question 17: What is the name of the user-installed (i.e. non-Apple) email app?

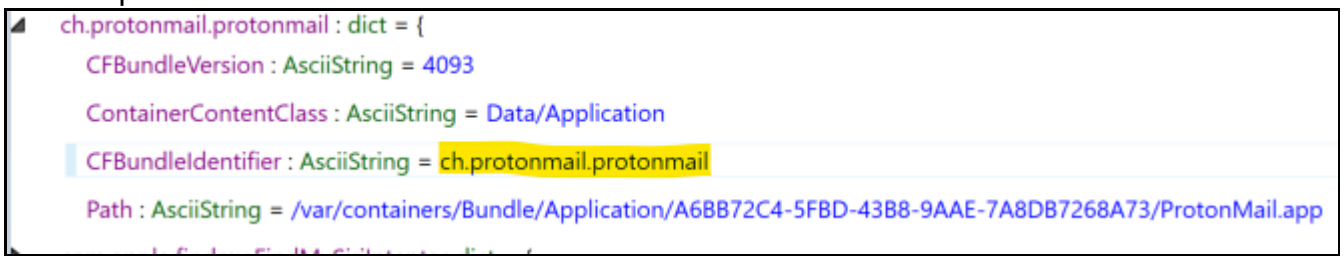
Consensus Result: ProtonMail

Expected Response Explanation:

Information about installed apps is stored in /Backup/Manifest.plist.

Expected Response Illustration:

Manifest.plist



Cellebrite "Installed Applications" table parsed from Manifest.plist (filtered)

TABLE 1

Question 18

Question 18: What is the version of the user-installed (i.e. non-Apple) email app?

Manufacturer's
Expected Response: 40.9.3

WebCode	Response
232E3H	1.11.17 (4093)
23R6RY	40.9.3
2MP2LK	1.11.17 (4093). - See comments [Table 2: Additional Comments] regarding this answer.
2U4K6K	40.9.3
2UJ7EL	40.9.3
2ZD34D	40.9.3
3LXYYV	v. 40.9.3
4KQATB	40.9.3
4VD9JG	40.9.3
6LKHCE	40.9.3
6R89XA	40.9.3
73ULRR	40.9.3
7FEZVR	40.9.3
7NZ8BH	40.9.3
7TZH7H	1.11.17
7WXYJC	40.9.3
82KA7F	40.9.3
8E9BN8	40.9.3
8FY44R	40.9.3
8XED4T	40.9.3
93EEZE	40.9.3
9AEVD6	40.9.3
9C38CB	1.11.17
9J3RE7	40.9.3
A8PRHD	40.9.3
AB3RE6	40.9.3
AJGDN9	40.9.3
AUEEZC	40.9.3
B7LJQ6	40.9.3

TABLE 1

Question 18	
WebCode	**Response**
BGDYWL	40.9.3
BK4CEC	1.11.17
CMVPWM	40.9.3
CTTKD8	1.11.17 (4093)
DDYEJ4	40.9.3
DGXQF4	40.9.3
DJL3EA	40.9.3
EKZT67	40.9.3
ET7TE8	40.9.3
FNQKQ8	40.9.3
FXKMCH	40.9.3
G3E42G	40.9.3
GA8EUY	40.9.3
GJTH2X	40.9.3
GXBBQ6	40.9.3
HBTH3W	1.11.17(4093)
HRJN96	40.9.3
JRWEYZ	40.9.3
KQZJPW	40.9.3
L2Z97X	40.9.3
L78WJY	40.9.3
LDRZQ3	1.11.17
LUED6U	40.9.3
MK4BJT	40.9.3
P94MFP	40.9.3
PBRYEU	40.9.3
PRFA2W	40.9.3
PVHA3U	40.9.3
PZYA29	40.9.3
Q9J39W	40.9.3
QBL2JP	3608.100.0.1.6

TABLE 1

Question 18	
WebCode	**Response**
QTQBNV	40.9.3
QZTKUN	40.9.3
RA9UVM	40.9.3
RWD889	40.9.3
T6DJYU	40.9.3
TGQJVM	40.9.3
TL2WDL	40.9.3
U2P8ZN	40.9.3
UCYFWG	40.9.3
UM9CJR	40.9.3
UPZBXQ	40.9.3
UQBAVK	40.9.3
UTYLUQ	version 40.9.3
V6M9DQ	40.9.3
VJC6V2	10.0
VU246Q	40.9.3
WJ3TAP	40.9.3
WX466N	40.9.3
X78WMG	40.9.3
X8ZRAP	40.9.3
XJGCUL	40.9.3
XY9AWG	40.9.3
XYELUY	40.9.3
YQ9AWF	1.11.17
Z8D34E	40.9.3
ZB38DY	40.9.3
ZX8VNE	40.9.3

TABLE 1

Question 18

Question 18: What is the version of the user-installed (i.e. non-Apple) email app?

Consensus Result: 40.9.3 and all formatting styles which represent the same information. In addition, 1.11.17 was also accepted as the version of the user-installed email app.

Expected Response Explanation:

Information about installed apps is stored in /Backup/Manifest.plist.

Expected Response Illustration:

Manifest.plist

Cellebrite "Installed Applications" table parsed from Manifest.plist (filtered)

ch.protonmail.protonmail.plist

TABLE 1

Question 19

Question 19: What is the email address associated with the user-installed (i.e. non-Apple) email app?

Manufacturer's Expected Response: jondaniel2020@protonmail.com

WebCode	Response
232E3H	jondaniel2020@protonmail.com
23R6RY	jondaniel2020@protonmail.com
2MP2LK	jondaniel2020@protonmail.com
2U4K6K	jondaniel2020@protonmail.com
2UJ7EL	jondaniel2020@protonmail.com
2ZD34D	jondaniel2020@protonmail.com
3LXYYV	jondaniel2020@protonmail.com
4KQATB	jondaniel2020@protonmail.com
4VD9JG	jondaniel2020@protonmail.com
6LKHCE	jondaniel2020@protonmail.com
6R89XA	jondaniel2020@protonmail.com
73ULRR	jondaniel2020@protonmail.com
7FEZVR	jondaniel2020@protonmail.com
7NZ8BH	jondaniel2020@protonmail.com
7TZH7H	jondaniel2020@protonmail.com
7WXYJC	jondaniel2020@protonmail.com
82KA7F	jondaniel2020@protonmail.com
8E9BN8	jondaniel2020@protonmail.com
8FY44R	jondaniel2020@protonmail.com
8XED4T	jondaniel2020@protonmail.com
93EEZE	jondaniel2020@protonmail.com
9AEVD6	jondaniel2020@protonmail.com
9C38CB	jondaniel2020@protonmail.com
9J3RE7	jondaniel2020@protonmail.com
A8PRHD	jondaniel2020@protonmail.com
AB3RE6	jondaniel2020@ protonmail.com
AJGDN9	jondaniel2020@protonmail.com
AUEEZC	jondaniel2020@protonmail.com
B7LJQ6	jondaniel2020@protonmail.com

TABLE 1

Question 19	
WebCode	**Response**
BGDYWL	jondaniel2020@protonmail.com
BK4CEC	jondaniel2020@protonmail.com
CMVPWM	Jondaniel2020@protonmail.com
CTTKD8	jondaniel2020@protonmail.com
DDYEJ4	jondaniel2020@protonmail.com
DGXQF4	jondaniel2020@protonmail.com
DJL3EA	jondaniel2020@protonmail.com
EKZT67	jondaniel2020@protonmail.com
ET7TE8	jondaniel2020@protonmail.com
FNQKQ8	jondaniel2020@protonmail.com
FXKMCH	jondaniel2020@protonmail.com
G3E42G	jondaniel2020@protonmail.com
GA8EUY	jondaniel2020@protonmail.com
GJTH2X	jondaniel2020@protonmail.com
GXBBQ6	jondaniel2020@protonmail.com
HBTH3W	jondaniel2020@protonmail.com
HRJN96	Jondaniel2020@protonmail.com
JRWEYZ	jondaniel2020@protonmail.com
KQZJPW	jondaniel2020@protonmail.com
L2Z97X	jondaniel2020@protonmail.com
L78WJY	jondaniel2020@protonmail.com
LDRZQ3	jondaniel2020@protonmail.com
LUED6U	jondaniel2020@protonmail.com
MK4BJT	jondaniel2020@protonmail.com
P94MFP	jondaniel2020@protonmail.com
PBRYEU	jondaniel2020@protonmail.com
PRFA2W	jondaniel2020@protonmail.com
PVHA3U	jondaniel2020@protonmail.com
PZYA29	jondaniel2020@protonmail.com
Q9J39W	jondaniel2020@protonmail.com
QBL2JP	jon.daniels39@icloud.com

TABLE 1

Question 19	
WebCode	**Response**
QTQBNV	jondaniel2020@protonmail.com
QZTKUN	Jondaniel2020@protonmail.com
RA9UVM	jondaniel2020@protonmail.com
RWD889	jondaniel2020@protonmail.com
T6DJYU	jondaniel2020@protonmail.com
TGQJVM	jondaniel2020@protonmail.com
TL2WDL	jondaniel2020@protonmail.com
U2P8ZN	jondaniel2020@protonmail.com
UCYFWG	jondaniel2020@protonmail.com
UM9CJR	jondaniel2020@protonmail.com
UPZBXQ	jondaniel2020@protonmail.com
UQBAVK	jondaniel2020@protonmail.com
UTYLUQ	jondaniel2020@protonmail.com
V6M9DQ	jondaniel2020@protonmail.com
VJC6V2	jondaniel2020@protonmail.com
VU246Q	jondaniel2020@protonmail.com
WJ3TAP	jondaniel2020@protonmail.com
WX466N	jondaniel2020@protonmail.com
X78WMG	jondaniel2020@protonmail.com
X8ZRAP	jondaniel2020@protonmail.com
XJGCUL	jondaniel2020@protonmail.com
XY9AWG	Jondaniel2020@protonmail.com
XYELUY	jondaniel2020@protonmail.com
YQ9AWF	jondaniel2020@protonmail.com
Z8D34E	jondaniel2020@protonmail.com
ZB38DY	jondaniel2020@protonmail.com
ZX8VNE	jondaniel2020@protonmail.com

TABLE 1

Question 19

Question 19: What is the email address associated with the user-installed (i.e. non-Apple) email app?

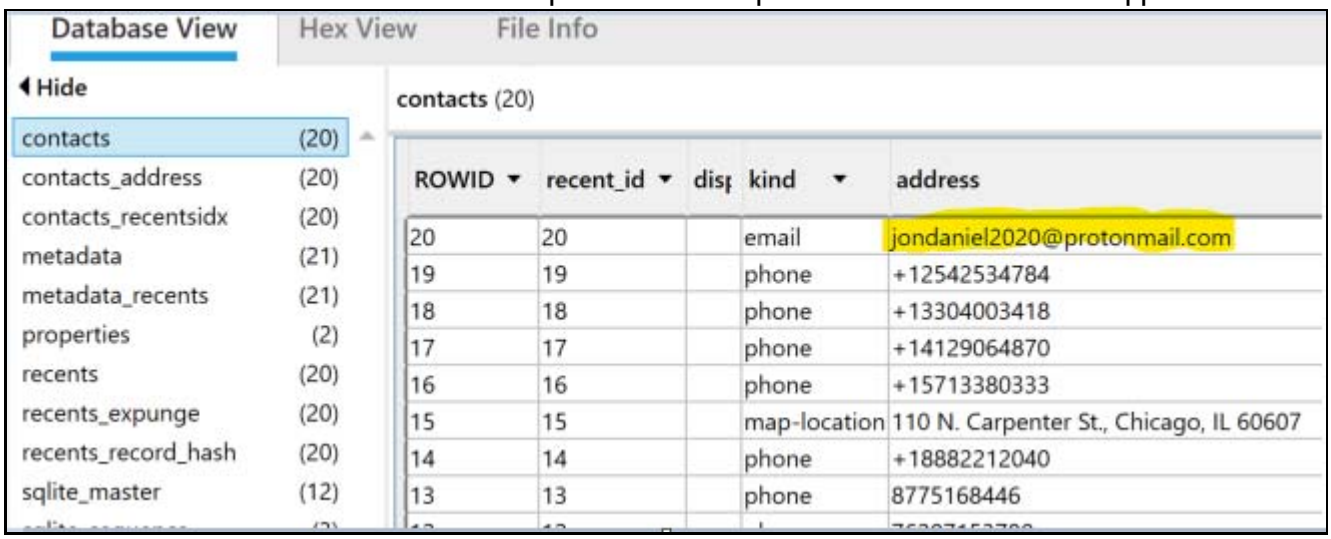
Consensus Result: jondaniel2020@protonmail.com

Expected Response Explanation:

Review of email messages or accounts on the device for protonmail will discover the above address in /mobile/Library/Recents/Recents or /mobile/Containers/Data/Application/com.tinginteractive.usms/Documents/10466320151241745810jondaniel2020.

Expected Response Illustration:

Database view of 10466320151241745810jondaniel2020 sqlite database for Protonmail app



Database view of 10466320151241745810jondaniel2020 sqlite database for Protonmail app

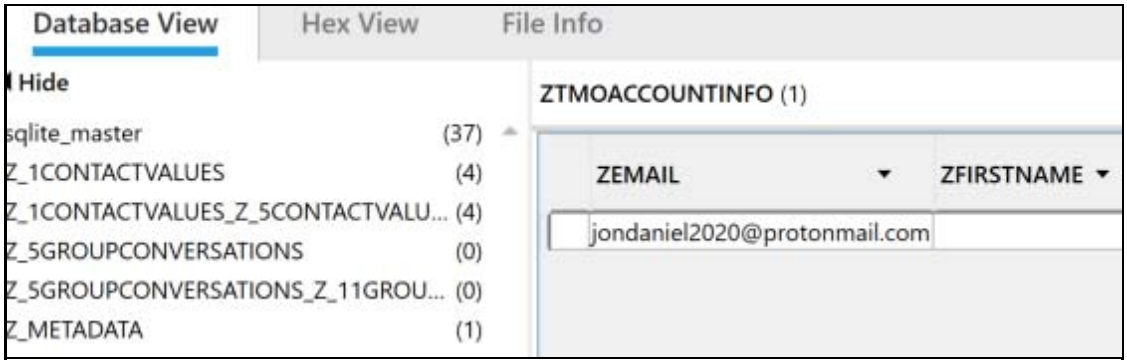


TABLE 1

Question 20

Question 20: What is the email address associated with the native (i.e. Apple) email app?

Manufacturer's Expected Response: jon.daniels39@icloud.com

WebCode	Response
232E3H	jon.daniels39@icloud.com
23R6RY	jon.daniels39@icloud.com
2MP2LK	jon.daniels39@icloud.com
2U4K6K	jon.daniels39@icloud.com
2UJ7EL	jon.daniels39@icloud.com
2ZD34D	jon.daniels39@icloud.com
3LXYYV	jon.daniels39@icloud.com
4KQATB	jon.daniels39@icloud.com
4VD9JG	jon.daniels39@icloud.com
6LKHCE	jon.daniels39@icloud.com
6R89XA	jon.daniels39@icloud.com
73ULRR	jon.daniels39@icloud.com
7FEZVR	jon.daniels39@icloud.com
7NZ8BH	jon.daniels39@icloud.com
7TZH7H	jon.daniels39@icloud.com
7WXYJC	jon.daniels39@icloud.com
82KA7F	jon.daniels39@icloud.com
8E9BN8	jon.daniels39@icloud.com
8FY44R	jon.daniels39@icloud.com
8XED4T	jon.daniels39@icloud.com
93EEZE	jon.daniels39@icloud.com
9AEVD6	jon.daniels39@icloud.com
9C38CB	jon.daniels39@icloud.com
9J3RE7	jon.daniels39@icloud.com
A8PRHD	jon.daniels39@icloud.com
AB3RE6	jon.daniels39@icloud.com
AJGDN9	Jon.daniels39@icloud.com
AUEEZC	jon.daniels39@icloud.com
B7LJQ6	jon.daniels39@icloud.com

TABLE 1

Question 20	
WebCode	**Response**
BGDYWL	jon.daniels39@icloud.com
BK4CEC	jon.daniels39@icloud.com
CMVPWM	jon.daniels39@icloud.com
CTTKD8	jon.daniels39@icloud.com
DDYEJ4	jon.daniels39@icloud.com
DGXQF4	jon.daniels39@icloud.com
DJL3EA	jon.daniels39@icloud.com
EKZT67	jon.daniels39@icloud.com
ET7TE8	jon.daniels39@icloud.com
FNQKQ8	jon.daniels39@icloud.com
FXKMCH	jon.daniels39@icloud.com
G3E42G	jon.daniels39@icloud.com
GA8EUY	jon.daniels39@icloud.com
GJTH2X	jon.daniels39@icloud.com
GXBBQ6	jon.daniels39@icloud.com
HBTH3W	jon.daniels39@icloud.com
HRJN96	Jon.daniels39@icloud.com
JRWEYZ	jon.daniels39@icloud.com
KQZJPW	jon.daniels39@icloud.com
L2Z97X	jon.daniels39@icloud.com
L78WJY	jon.daniels39@icloud.com
LDRZQ3	jon.daniels39@icloud.com
LUED6U	jon.daniels39@icloud.com
MK4BJT	jon.daniels39@icloud.com
P94MFP	jon.daniels39@icloud.com
PBRYEU	jon.daniels39@icloud.com
PRFA2W	jon.daniels39@icloud.com
PVHA3U	jon.daniels39@icloud.com
PZYA29	jon.daniels39@icloud.com
Q9J39W	jon.daniels39@icloud.com
QBL2JP	jon.daniels39@icloud.com

TABLE 1

Question 20	
WebCode	**Response**
QTQBNV	jon.daniels39@icloud.com
QZTKUN	jon.daniels39@icloud.com
RA9UVM	jon.daniels39@icloud.com
RWD889	jon.daniels39@icloud.com
T6DJYU	jon.daniels39@icloud.com
TGQJVM	jon.daniels39@icloud.com
TL2WDL	jon.daniels39@icloud.com
U2P8ZN	jon.daniels39@icloud.com
UCYFWG	jon.daniels39@icloud.com
UM9CJR	jon.daniels39@icloud.com
UPZBXQ	jon.daniels39@icloud.com
UQBAVK	jon.daniels39@icloud.com
UTYLUQ	jon.daniels39@icloud.com
V6M9DQ	jon.daniels39@icloud.com
VJC6V2	jon.daniels39@icloud.com
VU246Q	jon.daniels39@icloud.com
WJ3TAP	jon.daniels39@icloud.com
WX466N	jon.daniels39@icloud.com
X78WMG	jon.daniels39@icloud.com
X8ZRAP	jon.daniels39@icloud.com
XJGCUL	jon.daniels39@icloud.com
XY9AWG	Jondaniels39@icloud.com
XYELUY	jon.daniels39@icloud.com
YQ9AWF	jon.daniels39@icloud.com
Z8D34E	jon.daniels39@icloud.com
ZB38DY	jon.daniels39@icloud.com
ZX8VNE	Jon.daniels39@icloud.com

TABLE 1

Question 20

Question 20: What is the email address associated with the native (i.e. Apple) email app?

Consensus Result: jon.daniels39@icloud.com

Expected Response Explanation:

Information about application accounts on the device can be found in /mobile/Library/Accounts/Accounts3.sqlite or from reviewing the recent messages associated with the email app.

Expected Response Illustration:

Cellebrite "User Accounts" table (filtered)

6/15/2020 8:04:50 AM(U...	jon.daniels39@icloud.com	Account Description Game Center	
6/15/2020 8:05:02 AM(U...	jon.daniels39@icloud.com	Account Description IMAPMail	D3924A53-5128-4...
6/15/2020 8:05:02 AM(U...	jon.daniels39@icloud.com		446F3FE8-C5D1-43...

Database view of Accounts3.sqlite (Filtered)

bundle_identifier	sending_address	original_source	d
com.apple.mobilemail	jon.daniels39@icloud.com	com.apple.mobilemail	15
com.apple.MobileSMS	SMS:+12542534784	com.apple.MobileSMS	15

TABLE 1

Question 21

Question 21: How many unique SMS messages were RECEIVED FROM the phone number associated with the contact listed as "Mark"?

Manufacturer's Expected Response: 9

WebCode	Response
232E3H	9
23R6RY	9
2MP2LK	9
2U4K6K	9
2UJ7EL	9
2ZD34D	9
3LXYYV	8
4KQATB	9
4VD9JG	9
6LKHCE	9
6R89XA	9
73ULRR	10
7FEZVR	9
7NZ8BH	9
7TZH7H	9
7WXYJC	9
82KA7F	9
8E9BN8	9
8FY44R	9
8XED4T	9
93EEZE	9
9AEVD6	10
9C38CB	9
9J3RE7	9
A8PRHD	9
AB3RE6	9
AJGDN9	9
AUEEZC	9

TABLE 1

Question 21	
WebCode	**Response**
B7LJQ6	Nine
BGDYWL	10
BK4CEC	10
CMVPWM	9
CTTKD8	8
DDYEJ4	9
DGXQF4	9
DJL3EA	9
EKZT67	9
ET7TE8	10
FNQKQ8	9
FXKMCH	9
G3E42G	10
GA8EUY	10 (one blank)
GJTH2X	9
GXBBQ6	9
HBTH3W	9
HRJN96	Nine
JRWEYZ	9
KQZJPW	9
L2Z97X	9
L78WJY	9
LDRZQ3	9
LUED6U	9 unique SMS messages
MK4BJT	10
P94MFP	Nine
PBRYEU	9
PRFA2W	9
PVHA3U	9
PZYA29	9
Q9J39W	9

TABLE 1

Question 21	
WebCode	**Response**
QBL2JP	21
QTQBNV	9
QZTKUN	9
RA9UVM	Nine (9)
RWD889	9
T6DJYU	9
TGQJVM	9
TL2WDL	9
U2P8ZN	9
UCYFWG	9
UM9CJR	9
UPZBXQ	9
UQBAVK	8
UTYLUQ	9
V6M9DQ	9
VJC6V2	10
VU246Q	9
WJ3TAP	9
WX466N	9
X78WMG	9
X8ZRAP	9
XJGCUL	9
XY9AWG	9
XYELUY	10
YQ9AWF	9
Z8D34E	9
ZB38DY	9
ZX8VNE	25

TABLE 1

Question 21

Question 21: How many unique SMS messages were RECEIVED FROM the phone number associated with the contact listed as "Mark"?

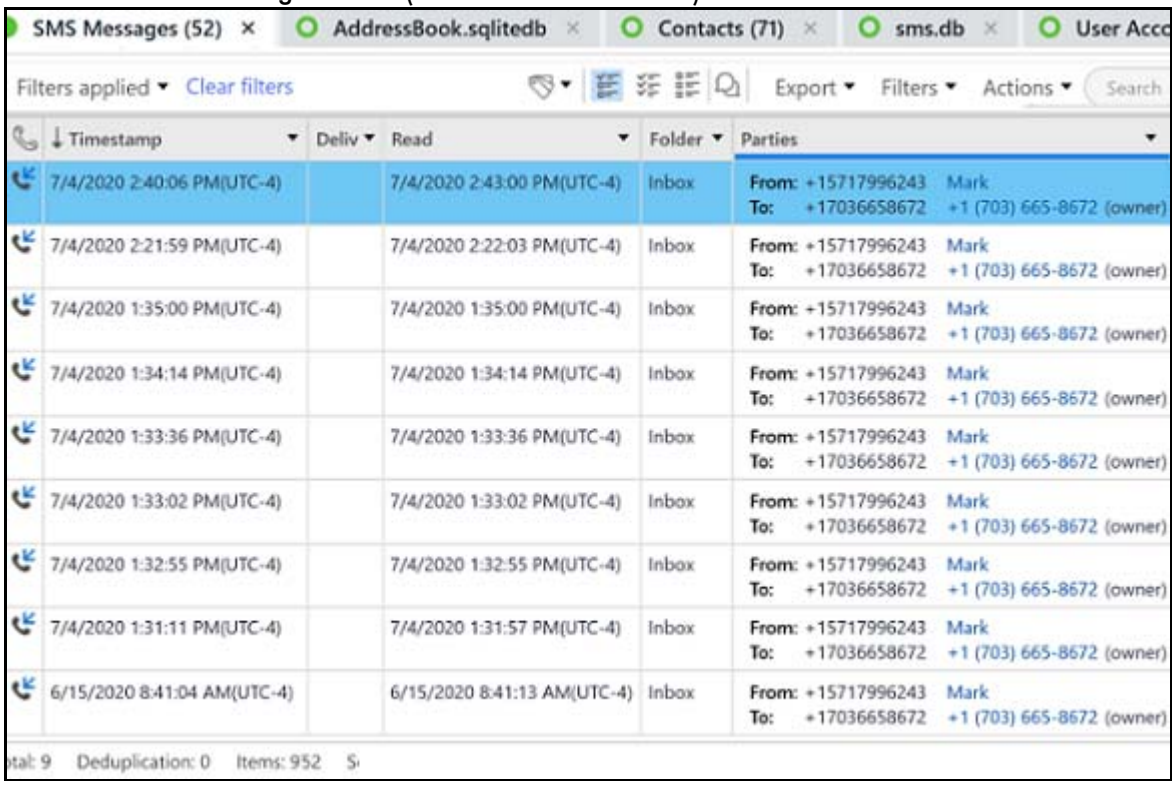
Consensus Result: 9

Expected Response Explanation:

Contact information for Mark is stored in /mobile/Library/AddressBook/AddressBook.sqlitedb which lists his number as +15717996243.
SMS Message information is stored in /mobile/Library/SMS/sms.db reviewing the database content and filtering by from: Mark finds nine messages from Mark.

Expected Response Illustration:

Cellebrite "SMS Messages" table (filtered for "from:Mark")



Other Responses:

Ten participants reported that there were 10 unique SMS messages. iOS keeps track of recent contacts in a database at /mobile/Library/Recents/Recents. If so configured, Cellebrite will include these records alongside those parsed from the communication storage files (e.g. SMS.db). These "recents" records are just pointers in the iOS that indicate a recent event for a particular contact. They are not records of additional (or unique) communications. Participants may have counted this "recent" record as a unique message, reporting a total of 10. Upon reviewing this record, one can see its folder is identified as "Recents" (not Inbox), it has an identical timestamp as another record, and has no content (body), nor a "To" party.

TABLE 1

Question 22

Question 22: How many unique unread SMS messages are on the phone?

Manufacturer's
Expected Response: 6

WebCode	Response
232E3H	6
23R6RY	6
2MP2LK	6
2U4K6K	6
2UJ7EL	6
2ZD34D	6
3LXYYV	1
4KQATB	6
4VD9JG	6
6LKHCE	6
6R89XA	6
73ULRR	6
7FEZVR	6
7NZ8BH	6
7TZH7H	6
7WXYJC	6
82KA7F	6
8E9BN8	6
8FY44R	6
8XED4T	6
93EEZE	6
9AEVD6	6
9C38CB	6
9J3RE7	6
A8PRHD	6
AB3RE6	6
AJGDN9	6
AUEEZC	6
B7LJQ6	Six

TABLE 1

Question 22	
WebCode	**Response**
BGDYWL	6
BK4CEC	6
CMVPWM	6
CTTKD8	17
DDYEJ4	6
DGXQF4	6
DJL3EA	6
EKZT67	24
ET7TE8	23
FNQKQ8	6
FXKMCH	6
G3E42G	6
GA8EUY	6 Unread messages
GJTH2X	6
GXBBQ6	6
HBTH3W	6
HRJN96	Six
JRWEYZ	6
KQZJPW	6
L2Z97X	6
L78WJY	6
LDRZQ3	6
LUED6U	6
MK4BJT	6
P94MFP	Six
PBRYEU	6
PRFA2W	6
PVHA3U	6
PZYA29	6
Q9J39W	6
QBL2JP	6

TABLE 1

Question 22	
WebCode	**Response**
QTQBNV	6
QZTKUN	6
RA9UVM	Six (6)
RWD889	6
T6DJYU	6
TGQJVM	6
TL2WDL	6
U2P8ZN	6
UCYFWG	6
UM9CJR	5
UPZBXQ	44
UQBAVK	6
UTYLUQ	6
V6M9DQ	6
VJC6V2	9
VU246Q	6
WJ3TAP	6
WX466N	6
X78WMG	6
X8ZRAP	6
XJGCUL	6
XY9AWG	6
XYELUY	6
YQ9AWF	6
Z8D34E	6
ZB38DY	6
ZX8VNE	6

TABLE 1

Question 22

Question 22: How many unique unread SMS messages are on the phone?

Consensus Result: 6

Expected Response Explanation:

SMS Message information is stored in /mobile/Library/SMS/sms.db. Reviewing the database content and filtering by Status: Unread finds six messages.

Expected Response Illustration:

Cellebrite "SMS Messages" table (filtered for "Status:Unread")

Folder	Parties	Body	Status
Inbox	From: 611 611 To: +17036658672 +1 (703) 665-8672 (owner)	Your Metro by T-Mobile authentication code is 308674. This co...	Unread
Inbox	From: +13304003418 To: +17036658672 +1 (703) 665-8672 (owner)	Your WhatsApp code: 726-437 You can also tap on this link to...	Unread
Inbox	From: +14129064870 To: +17036658672 +1 (703) 665-8672 (owner)	Your Signal verification code: 525-393 Or tap: sgnl://verify/525...	Unread
Inbox	From: 611 611 To: +17036658672 +1 (703) 665-8672 (owner)	Thanks for your $100.00 pymt on Acc 303846167. Conf 201177...	Unread
Inbox	From: 81961 To: +17036658672 +1 (703) 665-8672 (owner)	Your Apple ID Verification Code is: 010260	Unread
Inbox	From: 50472 To: +17036658672 +1 (703) 665-8672 (owner)	Your Apple ID Verification Code is: 185813	Unread

Total: 6 Deduplication: 0 Items: 6/52 Selected: 6

TABLE 1

Question 23

Question 23: Where did the device owner agree to meet on July 4?

Manufacturer's Expected Response: Lafayette Square

WebCode	Response
232E3H	Lafayette Square
23R6RY	Lafayette Square
2MP2LK	Lafayette square
2U4K6K	Lafayette square
2UJ7EL	Lafayette square
2ZD34D	Lafayette Square
3LXYYV	Lafayette square
4KQATB	Lafayette square
4VD9JG	Lafayette square
6LKHCE	Lafayette square
6R89XA	Lafayette square
73ULRR	Lafayette square
7FEZVR	Lafayette square
7NZ8BH	Lafayette square
7TZH7H	Lafayette square, WASHINGTON DC, U.S.A.
7WXYJC	Lafayette square
82KA7F	Lafayette square
8E9BN8	Lafayette square
8FY44R	Lafayette square
8XED4T	Lafayette square?
93EEZE	Lafayette square
9AEVD6	Lafayette square
9C38CB	Lafayette square
9J3RE7	DC, Lafayette square
A8PRHD	Lafayette Square
AB3RE6	Lafayette square
AJGDN9	Lafayette Square
AUEEZC	Lafayette square, DC
B7LJQ6	Lafayette square

TABLE 1

Question 23	
WebCode	**Response**
BGDYWL	Lafayette square
BK4CEC	Lafayette square
CMVPWM	Lafayette square?
CTTKD8	Lafayette square
DDYEJ4	Lafayette square
DGXQF4	Lafayette square
DJL3EA	Lafayette square
EKZT67	Lafayette square
ET7TE8	Lafayette square
FNQKQ8	Lafayette square
FXKMCH	Lafayette Square
G3E42G	Lafayette square
GA8EUY	Lafayette square
GJTH2X	Lafayette square
GXBBQ6	Lafayette square
HBTH3W	Lafayette square
HRJN96	Lafayette square?
JRWEYZ	Lafayette square
KQZJPW	Lafayette Square
L2Z97X	Lafayette square
L78WJY	Lafayette Square
LDRZQ3	Lafayette Square
LUED6U	Lafayette square
MK4BJT	Lafayette square
P94MFP	Lafayette square
PBRYEU	Lafayette Square
PRFA2W	Lafayette square
PVHA3U	Lafayette square
PZYA29	Lafayette square
Q9J39W	Lafayette square
QBL2JP	Lafayette square

TABLE 1

Question 23	
WebCode	**Response**
QTQBNV	Lafayette square
QZTKUN	Lafayette Square
RA9UVM	Lafayette square
RWD889	Lafayette Square in Washington, DC
T6DJYU	Lafayette square
TGQJVM	Lafayette Square
TL2WDL	Lafayette square
U2P8ZN	Lafayette square?
UCYFWG	Lafayette square
UM9CJR	Lafayette square
UPZBXQ	Lafayette square
UQBAVK	Lafayette square
UTYLUQ	Lafayette Square
V6M9DQ	Lafayette square
VJC6V2	Lafayette Square
VU246Q	Lafayette square
WJ3TAP	Lafayette square
WX466N	Lafayette square
X78WMG	Lafayette square
X8ZRAP	Lafayette Square
XJGCUL	Lafayette square
XY9AWG	Lafayette Square
XYELUY	Lafayette square
YQ9AWF	Lafayette Square
Z8D34E	Lafayette square
ZB38DY	Lafayette Square
ZX8VNE	Lafayette square

TABLE 1

Question 23

Question 23: Where did the device owner agree to meet on July 4?

Consensus Result: Lafayette square

Expected Response Explanation:

Review of SMS messages finds a conversation between the owner and Mark on July 4th in which they agree to meet in Lafayette square.

Expected Response Illustration:

Cellebrite "SMS Messages" table (selected entries from July 4)

	Sent	From: +17036658672 +1 (703) 665-8672 (owner) To: +15717996243 Mark	Yo
7/4/2020 1:31:57 PM(UTC-4)	Inbox	From: +15717996243 Mark To: +17036658672 +1 (703) 665-8672 (owner)	Yo U going to the thing in dc today?
	Sent	From: +17036658672 +1 (703) 665-8672 (owner) To: +15717996243 Mark	Idk. Not even sure what's going on. U?
7/4/2020 1:32:55 PM(UTC-4)	Inbox	From: +15717996243 Mark To: +17036658672 +1 (703) 665-8672 (owner)	Imma go down and look around.
7/4/2020 1:33:02 PM(UTC-4)	Inbox	From: +15717996243 Mark To: +17036658672 +1 (703) 665-8672 (owner)	May noy stay if its crowded
	Sent	From: +17036658672 +1 (703) 665-8672 (owner) To: +15717996243 Mark	Fair
	Sent	From: +17036658672 +1 (703) 665-8672 (owner) To: +15717996243 Mark	Where exactly? I could meet u
7/4/2020 1:33:36 PM(UTC-4)	Inbox	From: +15717996243 Mark To: +17036658672 +1 (703) 665-8672 (owner)	Lafayette square?
	Sent	From: +17036658672 +1 (703) 665-8672 (owner) To: +15717996243 Mark	Ok Maybe an hour or so...
	Sent	From: +17036658672 +1 (703) 665-8672 (owner) To: +15717996243 Mark	I'll hit I up

TABLE 1

Question 24

Question 24: What contact (name) has the phone number "202-762-1401" listed as a "Pager" number in the iOS address book?

Manufacturer's Expected Response: James Roberts

WebCode	Response
232E3H	James Roberts
23R6RY	James Roberts
2MP2LK	James Roberts - See Comments about different formatting of the phone number in question.
2U4K6K	James Roberts
2UJ7EL	James Roberts and Mark
2ZD34D	James Roberts
3LXYYV	James Roberts
4KQATB	James Roberts
4VD9JG	James Roberts
6LKHCE	James Roberts
6R89XA	James Roberts
73ULRR	James Roberts
7FEZVR	James Roberts
7NZ8BH	James Roberts
7TZH7H	James Roberts
7WXYJC	Mark
82KA7F	James Roberts
8E9BN8	James Roberts
8FY44R	James Roberts
8XED4T	James Roberts
93EEZE	James Roberts
9AEVD6	Mark
9C38CB	James Roberts
9J3RE7	James Roberts
A8PRHD	James Roberts
AB3RE6	James Roberts
AJGDN9	James Roberts
AUEEZC	James Roberts

TABLE 1

Question 24	
WebCode	**Response**
B7LJQ6	James Roberts
BGDYWL	James Roberts
BK4CEC	James Roberts
CMVPWM	James Roberts
CTTKD8	James Roberts
DDYEJ4	James Roberts
DGXQF4	James Roberts
DJL3EA	James Roberts
EKZT67	James Roberts
ET7TE8	James Roberts
FNQKQ8	James Roberts
FXKMCH	James Roberts
G3E42G	James Roberts
GA8EUY	James Roberts
GJTH2X	James Roberts
GXBBQ6	James Robert
HBTH3W	James Roberts
HRJN96	James Roberts
JRWEYZ	James Roberts
KQZJPW	Mark
L2Z97X	James Roberts (note: contact name Mark also has that pager number listed (12027621401))
L78WJY	James Roberts
LDRZQ3	James Roberts
LUED6U	James Roberts
MK4BJT	James Roberts
P94MFP	James Roberts
PBRYEU	James Roberts
PRFA2W	James Roberts
PVHA3U	James Roberts
PZYA29	James Roberts
Q9J39W	James Roberts

TABLE 1

Question 24	
WebCode	**Response**
QBL2JP	James Roberts
QTQBNV	James Roberts
QZTKUN	James Roberts
RA9UVM	James Roberts
RWD889	Mark
T6DJYU	James Roberts
TGQJVM	James Roberts
TL2WDL	James Roberts
U2P8ZN	James Roberts
UCYFWG	James Roberts
UM9CJR	James Roberts
UPZBXQ	James Roberts
UQBAVK	James Roberts
UTYLUQ	James Robert
V6M9DQ	James Roberts
VJC6V2	James Roberts
VU246Q	James Roberts
WJ3TAP	James Roberts
WX466N	James Roberts
X78WMG	James Roberts
X8ZRAP	James Roberts pager
XJGCUL	James Roberts
XY9AWG	James Roberts
XYELUY	Mark
YQ9AWF	James Roberts
Z8D34E	James Roberts
ZB38DY	James Roberts
ZX8VNE	There is no match to the pager number "202-762-1401", however, James Roberts and Mark both have this number prefixed with '1' stored as pager.

TABLE 1

Question 24

Question 24: What contact (name) has the phone number "202-762-1401" listed as a "Pager" number in the iOS address book?

Consensus Result: James Roberts (See the "Other Responses" section of the Summary Report, page 103.)

Expected Response Explanation:

Contact information is stored in /mobile/Library/AddressBook/AddressBook.sqlitedb. Review of this database for 202-762-1401 finds two entries with this number. A "Pager" number for James Roberts, and a "Home" Number for Mark.

Expected Response Illustration:

Cellebrite "Contacts" table showing entries containing 202-762-1401

Source file information	Name	Phones
AddressBook.sqlitedb : 0x20F16	James Roberts	General +17323388044 Pager (202) 762-1401
AddressBook.sqlitedb : 0x20E1B	Mark	General +15717996243 Home (202) 762-1401

Other Responses:

*Note: An entry in the database for the TextNow app (com.tinginteractive.usms) lists 202-762-1401 as the "home" number for Mark. Cellebrite PA 7.38.0.40 appears to be mis-mapping this field to "Pager" instead of "home". This should be taken into consideration when evaluating responses.

TABLE 1

Question 25

Question 25: What phone number did the phone miss a call from on June 24, 2020?

Manufacturer's
Expected Response: 12104087024

WebCode	Response
232E3H	+12104087024
23R6RY	+12104087024
2MP2LK	12104087024
2U4K6K	+1 (210) 408-7024
2UJ7EL	12104087024
2ZD34D	+1 (210) 408-7024
3LXYYV	1-210-408-7024
4KQATB	+1(210)4087024
4VD9JG	+12104087024
6LKHCE	+1 (210)408-7024
6R89XA	+1 (210) 408-7024
73ULRR	+12104087024
7FEZVR	12104087024
7NZ8BH	+1 (210) 408-7024
7TZH7H	+1(210)408-7024
7WXYJC	12104087024
82KA7F	+12104087024
8E9BN8	+1 (210) 408-7024
8FY44R	+1 (210) 408-7024
8XED4T	+12104087024
93EEZE	+1 (210) 408-7024
9AEVD6	+1 (210) 408-7024
9C38CB	+12104087024
9J3RE7	+12104087024
A8PRHD	2104087024
AB3RE6	+12104087024
AJGDN9	1-210-408-7024
AUEEZC	+12104087024
B7LJQ6	+12104087024

TABLE 1

Question 25	
WebCode	**Response**
BGDYWL	+1 (210) 408-7024
BK4CEC	+1 (210) 408-7024
CMVPWM	+1 (210) 408-7024
CTTKD8	+1 (210) 408-7024
DDYEJ4	12104087024
DGXQF4	+1 (210) 408-7024
DJL3EA	12104087024
EKZT67	+12104087024
ET7TE8	+12104087024
FNQKQ8	+12104087024
FXKMCH	+12104087024
G3E42G	+12104087024
GA8EUY	+1 (210) 408-7024
GJTH2X	1 (210) 408-7024
GXBBQ6	+12104087024
HBTH3W	+1 (210) 408-7024
HRJN96	+1 (210) 408-7024
JRWEYZ	+1 (210) 408-7024
KQZJPW	210-408-7024
L2Z97X	1 (210) 408-7024
L78WJY	210-408-7024
LDRZQ3	+12104087024
LUED6U	+1 (210) 408-7024
MK4BJT	+12104087024
P94MFP	+12104087024
PBRYEU	+12104087024
PRFA2W	+1(210)408-7024
PVHA3U	+1 (210)408-7024
PZYA29	+12104087024
Q9J39W	12104087024
QBL2JP	+1(210)408-7024

TABLE 1

Question 25	
WebCode	**Response**
QTQBNV	+1 (210) 408-7024
QZTKUN	1-210-408-7024
RA9UVM	+12104087024
RWD889	12104087024
T6DJYU	12104087024
TGQJVM	1(210) 408-7024
TL2WDL	+12104087024
U2P8ZN	+12104087024
UCYFWG	+12104087024
UM9CJR	+12104087024
UPZBXQ	+1 (210) 408-7024
UQBAVK	+12104087024
UTYLUQ	1(210)408-7024
V6M9DQ	+1 (210) 408-7024
VJC6V2	+12104087024
VU246Q	+12104087024
WJ3TAP	+12104087024
WX466N	+1 (210) 408-7024
X78WMG	+12104087024
X8ZRAP	1(210)408-7024
XJGCUL	+12104087024
XY9AWG	210-408-7024
XYELUY	+1 (210) 408-7024
YQ9AWF	+12104087024
Z8D34E	12104087024
ZB38DY	+12104087024
ZX8VNE	+12104087024

TABLE 1

Question 25

Question 25: What phone number did the phone miss a call from on June 24, 2020?

Consensus Result: 12104087024

Expected Response Explanation:

Call log data is stored in /mobile/Library/CallHistoryDB/CallHistory.storedata. A review of the log for calls on June 24, 2020 finds one missed call from 12104087024.

Expected Response Illustration:

Cellebrite "Call Log" table selection showing calls for June 24

Parties	Timestamp	Duration	Status	Cou
From: +13128009119 +1 (312) 800-9119	6/19/2020 9:39:05 AM(UTC-4)	00:00:00	Not answered	us
From: +15512850826 Scam Likely	6/19/2020 9:59:06 AM(UTC-4)	00:00:00	Not answered	us
From: +15512850826 Scam Likely	6/19/2020 9:59:11 AM(UTC-4)	00:00:00	Not answered	us
From: +15127984642 +1 (512) 798-4642	6/19/2020 2:54:46 PM(UTC-4)	00:00:00	Not answered	us
From: +12104087024 +1 (210) 408-7024	6/24/2020 2:14:21 PM(UTC-4)	00:00:00	Not answered	us
To: +15717996243 Mark	6/27/2020 1:10:58 PM(UTC-4)	00:00:00	Not answered	us

TABLE 1

Question 26

Question 26: What contact (name) called the phone on July 4, 2020 at 6:31 PM?

Manufacturer's
Expected Response: Mark

WebCode	Response
232E3H	Mark
23R6RY	Mark
2MP2LK	Mark
2U4K6K	Mark
2UJ7EL	Mark
2ZD34D	Mark
3LXYYV	Mark
4KQATB	Mark
4VD9JG	Mark
6LKHCE	Mark
6R89XA	Mark
73ULRR	Mark
7FEZVR	Mark
7NZ8BH	Mark
7TZH7H	Mark
7WXYJC	Mark
82KA7F	Mark
8E9BN8	Mark
8FY44R	Mark
8XED4T	Mark
93EEZE	Mark
9AEVD6	Mark
9C38CB	Mark
9J3RE7	Mark
A8PRHD	Mark
AB3RE6	Mark
AJGDN9	Mark
AUEEZC	Mark
B7LJQ6	Mark

TABLE 1

Question 26	
WebCode	**Response**
BGDYWL	Mark
BK4CEC	Mark
CMVPWM	Mark
CTTKD8	Mark
DDYEJ4	Mark
DGXQF4	Mark
DJL3EA	Mark
EKZT67	Mark
ET7TE8	Mark
FNQKQ8	Mark
FXKMCH	Mark
G3E42G	Mark
GA8EUY	Mark
GJTH2X	Mark
GXBBQ6	Mark
HBTH3W	Mark
HRJN96	Mark
JRWEYZ	Mark
KQZJPW	Mark
L2Z97X	Mark
L78WJY	Mark
LDRZQ3	Mark
LUED6U	Mark
MK4BJT	Mark
P94MFP	Mark
PBRYEU	Mark
PRFA2W	Mark
PVHA3U	Mark
PZYA29	Mark
Q9J39W	Mark
QBL2JP	Mark

TABLE 1

Question 26	
WebCode	**Response**
QTQBNV	Mark
QZTKUN	Mark
RA9UVM	Mark +15717996243
RWD889	Mark
T6DJYU	Mark
TGQJVM	Mark
TL2WDL	Mark
U2P8ZN	Mark
UCYFWG	Mark
UM9CJR	Mark
UPZBXQ	Mark
UQBAVK	Mark
UTYLUQ	Mark
V6M9DQ	Mark
VJC6V2	“Mark”
VU246Q	Mark
WJ3TAP	Mark
WX466N	Mark
X78WMG	Mark
X8ZRAP	Mark
XJGCUL	Mark
XY9AWG	Mark
XYELUY	Mark
YQ9AWF	Mark
Z8D34E	Mark
ZB38DY	Mark
ZX8VNE	Mark

TABLE 1

Question 26

Question 26: What contact (name) called the phone on July 4, 2020 at 6:31 PM?

Consensus Result: Mark

Expected Response Explanation:

Call log data is stored in /mobile/Library/CallHistoryDB/CallHistory.storedata. Review of the log for calls on July 4, 2020 at 6:31 PM identifies the caller as Mark.

Expected Response Illustration:

Cellebrite "Call Log" table selection showing call on July 4, 2020 at 6:31 PM

TABLE 1

Question 27

Question 27: How many outgoing calls were made from this phone?

Manufacturer's
Expected Response: 5

WebCode	Response
232E3H	5
23R6RY	5
2MP2LK	5
2U4K6K	5
2UJ7EL	5
2ZD34D	5
3LXYYV	5
4KQATB	5
4VD9JG	5
6LKHCE	5
6R89XA	5
73ULRR	5
7FEZVR	5
7NZ8BH	5
7TZH7H	5
7WXYJC	5
82KA7F	5
8E9BN8	5 (1 Answered and 4 unanswered)
8FY44R	5
8XED4T	5
93EEZE	5
9AEVD6	5
9C38CB	5
9J3RE7	5
A8PRHD	5
AB3RE6	5
AJGDN9	5
AUEEZC	5
B7LJQ6	Five

TABLE 1

Question 27	
WebCode	**Response**
BGDYWL	5
BK4CEC	5
CMVPWM	10
CTTKD8	5
DDYEJ4	5
DGXQF4	5
DJL3EA	5
EKZT67	5
ET7TE8	5
FNQKQ8	5
FXKMCH	5
G3E42G	5
GA8EUY	5
GJTH2X	5
GXBBQ6	5
HBTH3W	5
HRJN96	Five
JRWEYZ	5
KQZJPW	5 including 4 cancelled calls
L2Z97X	5
L78WJY	5
LDRZQ3	5
LUED6U	5
MK4BJT	5
P94MFP	Five
PBRYEU	5
PRFA2W	5
PVHA3U	5
PZYA29	5
Q9J39W	5
QBL2JP	5

TABLE 1

Question 27	
WebCode	**Response**
QTQBNV	5
QZTKUN	5
RA9UVM	Five (5)
RWD889	5
T6DJYU	5
TGQJVM	5
TL2WDL	5
U2P8ZN	5
UCYFWG	5
UM9CJR	5
UPZBXQ	5
UQBAVK	5
UTYLUQ	5
V6M9DQ	5
VJC6V2	5
VU246Q	5
WJ3TAP	5
WX466N	5
X78WMG	5
X8ZRAP	5
XJGCUL	5
XY9AWG	5
XYELUY	5
YQ9AWF	5
Z8D34E	5
ZB38DY	4
ZX8VNE	5

TABLE 1

Question 27

Question 27: How many outgoing calls were made from this phone?

Consensus Result: 5

Expected Response Explanation:

Call log data is stored in /mobile/Library/CallHistoryDB/CallHistory.storedata. Filtering the list for outgoing calls results in five calls.

Expected Response Illustration:

Cellebrite "Call Log" table selection showing outgoing calls

Parties	Timestamp
To: +15717996243 Mark	6/27/2020 1:10:58 PM(UTC-4)
To: +15717996243 Mark	7/4/2020 6:29:11 PM(UTC-4)
To: 2022823030 2022823030	7/4/2020 6:38:15 PM(UTC-4)
To: 2027157707 2027157707	7/4/2020 6:38:56 PM(UTC-4)
To: +15717996243 Mark	7/4/2020 6:28:32 PM(UTC-4)

TABLE 1

Question 28

Question 28: What was the date and time of the LAST outgoing call? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset).

Manufacturer's Expected Response: 07/04/2020 06:38 PM (UTC-4)

WebCode	Response
232E3H	07/04/2020 06:38 PM (UTC-4)
23R6RY	07/04/2020 06:38 PM (UTC-4)
2MP2LK	07/04/2020 18:38 (UTC -4)
2U4K6K	04/07/2020 6:38 PM (UTC-4)
2UJ7EL	07/04/2020 06:38:56 PM (UTC-4)
2ZD34D	07/04/2020 18:38:56pm(UTC-4)
3LXYYV	07/04/2020 17:38 PM (UTC -5)
4KQATB	07/04/2020 18:38 PM
4VD9JG	07/04/2020 06:38 PM (UTC-4)
6LKHCE	07/04/2020 06:38 PM (UTC-4)
6R89XA	7.04.2020 06:38:56 pm (UTC-4)
73ULRR	07/04/2020 06:38 PM (UTC-4)
7FEZVR	07/04/2020 06:38 PM (UTC-4)
7NZ8BH	07/04/2020 06:38 PM
7TZH7H	07/04/2020 06:38 PM (UTC-4)
7WXYJC	07/04/2020 06:38 PM
82KA7F	07/04/2020 10:38 pm (UTC+0)
8E9BN8	07/04/2020 06:38:56 PM (UTC-4)
8FY44R	7/4/2020 6:38:56 PM(UTC-4)
8XED4T	7/4/2020 6:38:56 PM(UTC-4)
93EEZE	07/04/2020 06:38 PM(UTC-4)
9AEVD6	07/04/2020, 06:38:56 PM (UTC-4)
9C38CB	07/04/2020 06:38 PM (UTC-4)
9J3RE7	07/04/2020 18:38 PM (UTC-4)
A8PRHD	07/04/2020 18:38 PM (UTC -4)
AB3RE6	07/04/2020 06:38 PM (UTC-4)
AJGDN9	07/04/2020 06:38 PM (UTC -4)
AUEEZC	07/04/2020 06:38 PM (UTC-4)

TABLE 1

Question 28	
WebCode	**Response**
B7LJQ6	07/04/2020 18:38 PM
BGDYWL	07/04/2020 06:38 PM (UTC-4)
BK4CEC	07/04/2020 06:38 PM (UTC-4)
CMVPWM	07/05/2020 13:51:24 PM (UTC-4)
CTTKD8	07/04/2020 06:38 PM (UTC-4)
DDYEJ4	07/04/2020 06:38 PM (UTC-4)
DGXQF4	07/04/2020 06:38 PM(UTC-4)
DJL3EA	7/4/2020 6:38 PM(UTC-4)
EKZT67	07/04/2020 06:38 PM (UTC-4)
ET7TE8	07/04/2020 18:38 (UTC-4) PM
FNQKQ8	07/04/2020 06:38:56 PM (0x3793)
FXKMCH	07/04/2020 06:38 PM (UTC-4)
G3E42G	7/4/2020 6:38:56 PM(UTC-4)
GA8EUY	07/04/2020 18:38:56 PM (UTC-4)
GJTH2X	07/04/2020 6:38 PM (UTC-4)
GXBBQ6	07/04/2020 06:38 PM (UTC-4)
HBTH3W	07/04/2020 06:38 PM (UTC-4)
HRJN96	07/04/2020 17:38(UTC-5)
JRWEYZ	07/04/2020 06:38 PM (UTC-4)
KQZJPW	07/04/2020 06:38 PM(UTC-4)
L2Z97X	7/4/2020 18:38(UTC-4)
L78WJY	07/04/2020 06:38:56PM (UTC-4)
LDRZQ3	07/04/2020 06:38 PM (UTC-4)
LUED6U	07/04/2020 06:38 PM (UTC-4)
MK4BJT	07/04/2020 06:38 PM (UTC-4)
P94MFP	7/4/2020 6:38:56 PM(UTC-4)
PBRYEU	07/04/2020 06:38 PM (UTC -4:00)
PRFA2W	07/04/2020 18:38 PM (UTC -4)
PVHA3U	07/04/2020 6:38:56 PM (UTC -4)
PZYA29	07/04/2020 06:38 PM(UTC-4)
Q9J39W	07/04/2020 06:38 PM (UTC-4)

TABLE 1

Question 28	
WebCode	**Response**
QBL2JP	07/04/2020 06:38 PM (UTC-4)
QTQBNV	7/4/2020 18:38(UTC-4)
QZTKUN	07/04/2020 at 06:38 PM (UTC-4)
RA9UVM	07/04/2020 10:38 PM, offset 0x3793
RWD889	07/04/2020 06:38:56 PM (UTC-4)
T6DJYU	07/04/2020 06:38 PM (UTC-4)
TGQJVM	06/27/20 10:10:58 AM (UTC-7)
TL2WDL	7/4/2020 6:38 PM(UTC-4)
U2P8ZN	07/04/2020 06:38 PM (UTC-4)
UCYFWG	07/04/2020 6:38 PM(UTC-4)
UM9CJR	7/4/2020 6:38:56 PM (UTC-4)
UPZBXQ	07/04/2020 06:38 PM(UTC-4)
UQBAVK	07/04/2020 17:38 (UTC-5)
UTYLUQ	07/04/2020 6:38 PM (UTC -4)
V6M9DQ	7/4/2020 6:38 PM (UTC-4)
VJC6V2	7/4/2020 6:38:56 PM(UTC-4)
VU246Q	07/4/2020 06:38 PM (UTC-4)
WJ3TAP	7/4/2020 6:38:56 PM(UTC-4)
WX466N	07/04/2020 6:38 PM (UTC-4)
X78WMG	07/04/2020 06:38(UTC-4) PM
X8ZRAP	07/04/2020 06:38 PM (UTC-4)
XJGCUL	07/04//2020 06:38 PM (UTC-4)
XY9AWG	7/4/2020 6:38 PM (UTC -4)
XYELUY	7/4/2020 6:38:56 PM (UTC-4)
YQ9AWF	07/04/2020 18:38PM (UTC-4) or 6:38PM (UTC-4)
Z8D34E	7/4/2020 6:38 PM(UTC-4)
ZB38DY	7/4/2020 6:38:15 PM(UTC-4)
ZX8VNE	07/04/2020 06:38 PM (UTC-4)

TABLE 1

Question 28

Question 28: What was the date and time of the LAST outgoing call? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset).

Consensus Result: 07/04/2020 06:38 PM (UTC-4) and all formatting styles including different time zones which represent the same information.

Expected Response Explanation:

Call log data is stored in /mobile/Library/CallHistoryDB/CallHistory.storedata. Filtering the list for outgoing calls and sorting by timestamp identifies the last call placed at 07/04/2020 06:38:56 PM(UTC-4).

Expected Response Illustration:

Cellebrite "Call Log" table selection showing outgoing calls

Parties	Timestamp
To: +15717996243 Mark	6/27/2020 1:10:58 PM(UTC-4)
To: +15717996243 Mark	7/4/2020 6:29:11 PM(UTC-4)
To: 2022823030 2022823030	7/4/2020 6:38:15 PM(UTC-4)
To: 2027157707 2027157707	7/4/2020 6:38:56 PM(UTC-4)
To: +15717996243 Mark	7/4/2020 6:28:32 PM(UTC-4)

TABLE 1

Question 29

Question 29: With what service or application is the number 2029459404 associated?

Manufacturer's Expected Response: TextNow

WebCode	Response
232E3H	TextNow
23R6RY	TextNow
2MP2LK	TextNow
2U4K6K	TextNow
2UJ7EL	TextNow
2ZD34D	ProtonMail
3LXYYV	TextNow
4KQATB	Textnow
4VD9JG	TextNow
6LKHCE	TextNow
6R89XA	TextNow
73ULRR	TextNow
7FEZVR	TextNow
7NZ8BH	TextNow
7TZH7H	TextNow
7WXYJC	TextNow
82KA7F	TextNow
8E9BN8	TextNow
8FY44R	TextNow
8XED4T	TextNow
93EEZE	TextNow
9AEVD6	ProtonMail
9C38CB	TextNow
9J3RE7	TextNow
A8PRHD	TextNow
AB3RE6	ProntonMail
AJGDN9	ProtonMail
AUEEZC	TextNow
B7LJQ6	TextNow

TABLE 1

Question 29	
WebCode	**Response**
BGDYWL	TextNow
BK4CEC	Protonmail
CMVPWM	TextNow
CTTKD8	TextNow
DDYEJ4	ProtonMail
DGXQF4	TextNow
DJL3EA	TextNow
EKZT67	TextNow
ET7TE8	TextNow
FNQKQ8	TextNow
FXKMCH	TextNow
G3E42G	TextNow
GA8EUY	TextNow
GJTH2X	TextNow
GXBBQ6	TextNow
HBTH3W	TextNow
HRJN96	TextNow
JRWEYZ	TextNow
KQZJPW	ProtonMail
L2Z97X	TextNow
L78WJY	TextNow
LDRZQ3	TextNow
LUED6U	TextNow
MK4BJT	TextNow
P94MFP	TextNow
PBRYEU	TextNow
PRFA2W	TextNow
PVHA3U	TextNow
PZYA29	TextNow
Q9J39W	TextNow
QBL2JP	tinginteractive.usms

TABLE 1

Question 29	
WebCode	**Response**
QTQBNV	TextNow
QZTKUN	TextNow
RA9UVM	iOS Textnow (com.tinginteractive.usms)
RWD889	TextNow
T6DJYU	TextNow
TGQJVM	ProtonMail
TL2WDL	TextNow
U2P8ZN	TextNow
UCYFWG	TextNow
UM9CJR	TextNow
UPZBXQ	TextNow
UQBAVK	Protonmail.com
UTYLUQ	Text Now
V6M9DQ	TextNow
VJC6V2	Protonmail
VU246Q	TextNow
WJ3TAP	TextNow
WX466N	TextNow
X78WMG	TextNow
X8ZRAP	Textnow
XJGCUL	TextNow
XY9AWG	TextNow
XYELUY	TextNow
YQ9AWF	TextNow
Z8D34E	ProtonMail
ZB38DY	TextNow
ZX8VNE	Proton Mail

TABLE 1

Question 29

Question 29: With what service or application is the number 2029459404 associated?

Consensus Result: TextNow

Expected Response Explanation:

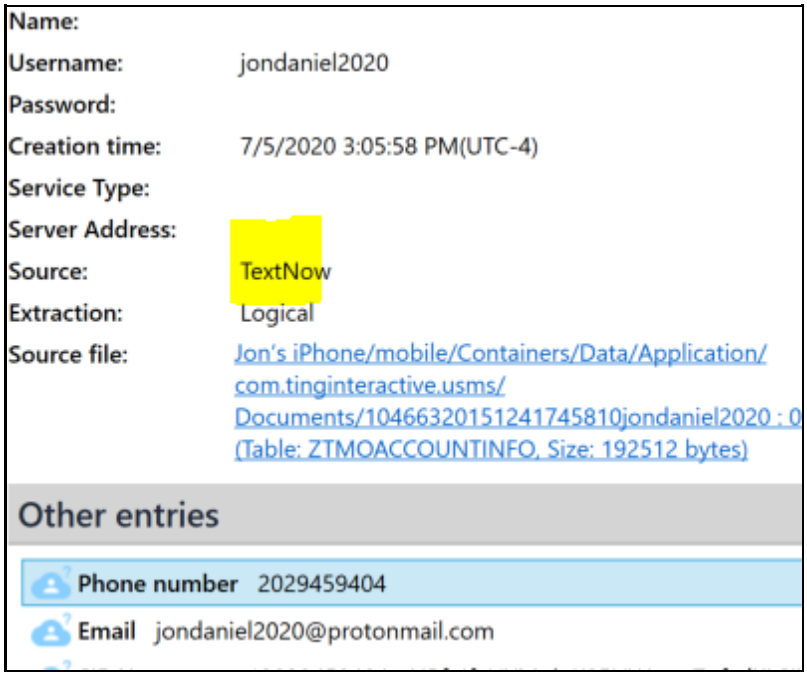
2029459404 is a 10-digit phone number. A search of User accounts (or a global search) for this number discovers it to be the phone number of the record for the jondaniel2020 TextNow account, as noted in /mobile/Containers/Data/Application/com.tinginteractive.usms/Documents/10466320151241745810jondaniel2020.

Expected Response Illustration:

Search hit for 2029459404 in com.tinginteractive.usms/~...jondaniel2020 database

Offset	Length	Value	Source
0x5E49	0x8	UserAccount.TimeCreated: 7/5/2020 3:05:58 PM(UTC-4)	/mobile/Containers...
0x5E71	0x1C	UserAccount.EmailAddress.Value: jondaniel2020@protonmail.com	/mobile/Containers...
0x5E8D	0xA	UserAccount.PhoneNumber.Value: 2029459404	/mobile/Containers...
0x5EAC	0x20	UserAccount.UserID.Value: a3b48df1d69d6e1f7694bef3569fda44	/mobile/Containers...
0x5ECC	0x38	UserAccount.UserID.Value: 12029459404_sNPfyJfeUYMnjnK95HWoxwZpfxdKLSIXX4O6Faqznz5R	/mobile/Containers...
0x5F18	0xD	UserAccount.Username: jondaniel2020	/mobile/Containers...

Cellebrite Contact card containing 2029459404



Other Responses:

Twelve participants reported Protonmail. The phone number 2029459404 is assigned to/by/for the TextNow application/service. Cellebrite identifies the username and other information associated with the TextNow app, including the email used to register the account, jondaniel2020@protonmail.com. There are no records of this phone number in the configuration or account information for the ProtonMail app.

TABLE 1

Question 30

Question 30: What health-related app did the user install?

Manufacturer's Expected Response: Renpho

WebCode	Response
232E3H	Renpho
23R6RY	Renpho
2MP2LK	Renpho
2U4K6K	Renpho
2UJ7EL	Renpho
2ZD34D	Renpho
3LXYYV	Renpho
4KQATB	Renpho
4VD9JG	Renpho
6LKHCE	Renpho
6R89XA	Renpho
73ULRR	Renpho
7FEZVR	Renpho
7NZ8BH	Health, Renpho
7TZH7H	Renpho
7WXYJC	Renpho
82KA7F	Renpho
8E9BN8	Renpho
8FY44R	Renpho
8XED4T	Renpho
93EEZE	Renpho
9AEVD6	Renpho
9C38CB	Renpho
9J3RE7	Renpho
A8PRHD	Renpho
AB3RE6	Renpho
AJGDN9	RenPho
AUEEZC	Renpho
B7LJQ6	Renpho

TABLE 1

Question 30	
WebCode	**Response**
BGDYWL	Renpho
BK4CEC	Renpho
CMVPWM	Renpho
CTTKD8	Renpho
DDYEJ4	Renpho
DGXQF4	RenPho
DJL3EA	Renpho
EKZT67	Renpho
ET7TE8	Renpho
FNQKQ8	Renpho
FXKMCH	Renpho
G3E42G	Renpho
GA8EUY	Renpho
GJTH2X	Renpho
GXBBQ6	RENPHO
HBTH3W	Renpho
HRJN96	Renpho
JRWEYZ	Renpho
KQZJPW	Renpho
L2Z97X	Renpho
L78WJY	Renpho
LDRZQ3	Renpho
LUED6U	Renpho
MK4BJT	Renpho
P94MFP	Health
PBRYEU	Renpho
PRFA2W	Renpho
PVHA3U	Renpho
PZYA29	Renpho
Q9J39W	Renpho
QBL2JP	Health Privacy Service

TABLE 1

Question 30	
WebCode	**Response**
QTQBNV	Renpho
QZTKUN	Renpho
RA9UVM	Apple Health
RWD889	Renpho
T6DJYU	Renpho
TGQJVM	Renpho
TL2WDL	Renpho
U2P8ZN	Renpho
UCYFWG	Renpho
UM9CJR	Renpho
UPZBXQ	Renpho
UQBAVK	Renpho
UTYLUQ	Health
V6M9DQ	Renpho
VJC6V2	Renpho
VU246Q	Renpho
WJ3TAP	Renpho
WX466N	Renpho
X78WMG	Renpho
X8ZRAP	Renpho
XJGCUL	Renpho
XY9AWG	Renpho
XYELUY	Renpho
YQ9AWF	Renpho
Z8D34E	Renpho
ZB38DY	Health
ZX8VNE	Renpho

TABLE 1

Question 30

Question 30: What health-related app did the user install?

Consensus Result: Renpho

Expected Response Explanation:

Information about installed applications is stored in /Backup/Manifest.plist. Reviewing this file finds two health and fitness related apps: Apple "Health," and Renpho. The Apple "Health" app is pre-installed on the iphone therefore not installed by the user.

Expected Response Illustration:

Manifest.plist

TABLE 1

Question 31

Question 31: Describe the content of the file with MD5 Hash a17ff17faf23d3fa09b943c7b530d24f.

Manufacturer's Expected Response: Rick Roll, Rick Astley, Never Gonna Give You Up, Music Video

WebCode	Response
232E3H	"Never Gonna Give You Up" music video
23R6RY	.MOV movie file containing Rick Astley strutting his funky stuff. "Never gonna give you up"
2MP2LK	Rick Astley - Never Gonna Give You Up (Video), commonly referred to as a "Rick Roll"
2U4K6K	Rick Astley - Never Gonna Give You Up
2UJ7EL	.MOV file playing a music video
2ZD34D	Rick Astley Never Gonna Give You Up Music Video
3LXYYV	Rick Astley dancing in a music video
4KQATB	Never gonna give you up (Rick Astley) musical Video
4VD9JG	It is a music video of Rick Astley's "Never Going to Give You Up".
6LKHCE	Rick Astley's "Never Gonna Give You Up" music video
6R89XA	A man singing a song.
73ULRR	Video file with a name of IMG_0052.MOV
7FEZVR	Music video of Rick Astley Never Gonna Give You Up
7NZ8BH	IMG_0053.MOV, IMG_0051.MOV, IMG_0052.MOV music video: Rick Astley - Never Gonna Give You Up
7TZH7H	Video Clip (Rick Astley - Never Gonna Give You Up)
7WXYJC	Never Gonna Give You Up music video by Rick Astley.
82KA7F	video clip (song)
8E9BN8	Movie file of Rick Astley,16676393 bytes in size
8FY44R	Video File of a music video. Rick Astley - Never Gonna Give You Up (Video)
8XED4T	Music Video, Never Gonna Give You Up...by Rick Astley
93EEZE	Video file, music video
9AEVD6	IMG_0052.MOV
9C38CB	It is a video file - video clip of Rick Astley, never gonna give you up
9J3RE7	Rickroll video
A8PRHD	A viral video known as "RickRolling" or "Never Gonna Give You Up by Rick Astley" (Nice)
AB3RE6	Music video of Rick Astley's "Never Gonna Give You Up" lasting 3m 32s
AJGDN9	This is a music video approximately 3 minutes and 32 seconds in length of Rick Astley singing "Never gonna give you up" which is commonly known as a "Rick Roll"
AUEEZC	Music Video

TABLE 1

Question 31	
WebCode	**Response**
B7LJQ6	Music Video - Rick Astley – Never gonna give you up.
BGDYWL	Rick Astley - Never Gonna Give You Up - Music Video
BK4CEC	music video clip
CMVPWM	Video file of Rick Astley singing Never Gonna Give You Up
CTTKD8	Rick Astley music video
DDYEJ4	Rick Astley Never Gonna Give You Up
DGXQF4	Rick Astley never gonna give you up video. "rickrolled"
DJL3EA	music video for Rick Astley "Never Gonna Give You Up"
EKZT67	Rick Astley music video
ET7TE8	IMG_0052.MOV video clip (Rick Astley Never Gonna Give you Up)
FNQKQ8	Music Video: Rick Astley-"Never gonna give you up"
FXKMCH	Music Artist, Rick Astley singing song, "Never gonna give you up" while dancing.
G3E42G	Music video Rick Astley Never Gonna give you up
GA8EUY	A music video with file name IMG_0052.MOV
GJTH2X	The content of that file is the music video for "Never Gonna Give You Up" by Rick Astley.
GXBBQ6	A music video of Never Gonna Give You Up by Rick Astley
HBTH3W	Rich Astley – "Never Gonna Give You Up" music video (IMG_0052.mov)
HRJN96	Appears to be a music video. To the song Never Gonna Give You up by Nick Astley
JRWEYZ	Video file
KQZJPW	Video file - music video of Rick Astley - Never Gonna Give You Up
L2Z97X	The Rick Roll music video.
L78WJY	Music Video
LDRZQ3	Never Gonna Give You Up music video by Rick Astley
LUED6U	This is a music video
MK4BJT	Music video. Never Gonna Give You Up
P94MFP	A music video titled Never Gonna Give You Up by Rick Astley
PBRYEU	Never Gonna Give You Up - Rick Astley
PRFA2W	music video in mov video file
PVHA3U	The content of the file is a music video of Rick Astley's "Never Gonna Give You Up".
PZYA29	Rick Astley - Never Gonna Give you up music video
Q9J39W	Rick Astley's official music video for "Never Gonna Give You Up"

TABLE 1

Question 31	
WebCode	**Response**
QBL2JP	Video IMG_0052.MOV
QTQBNV	This hash is associated with a video file named IMG_0052.MOV. It contains a music video typically used in rickrolling
QZTKUN	Music video by Rick Astley “Never Gonna Give You Up”
RA9UVM	Song: „We're no strangers to love You know the rules and so do I A full commitment's what I'm thinking of You wouldn't get this from any other guy“
RWD889	Music video by Rick Ashley for his song titled "Never Gonna Give You Up"
T6DJYU	Rick Astley - Never Gonna Give You Up (music video)
TGQJVM	Music Video
TL2WDL	Music video of the artist Rick Astley
U2P8ZN	A video file of Rick Astley singing Never Gonna Give You Up
UCYFWG	A music video for Rick Astley's song "Never Gonna Give You Up"
UM9CJR	Video file with audio
UPZBXQ	It is a .mov file. A music video
UQBAVK	Rick Astley music Video
UTYLUQ	Rick Astley - "Never Gonna Give You Up" Music Video
V6M9DQ	The file appears to be the Rick Astley – Never Gonna Give You Up music video.
VJC6V2	Being Rick-Roll’d by CTS during a competency exam, thank you!
VU246Q	Music video clip
WJ3TAP	.MOV Rick Astley Never gonna give you up. AKA Rickrolled
WX466N	Music video “Never Gonna Give You Up” by Rick Astley
X78WMG	Rick Astley-Never Gonna Give You Up, Video Clip. IMG_0052.MOV
X8ZRAP	Rick Astley Never Gonna give you up music video
XJGCUL	Music Video
XY9AWG	A Music video
XYELUY	Music video for the song "Never Gonna Give You Up" by Rick Astley
YQ9AWF	A music video of Rich Astley singing "Never Gonna Give You Up"
Z8D34E	Music video
ZB38DY	Rick Astley - Never Gonna Give You Up Video
ZX8VNE	Rick Astley music video never gonna give you up

TABLE 1

Question 31

Question 31: Describe the content of the file with MD5 Hash a17ff17faf23d3fa09b943c7b530d24f.

Consensus Result: A music video containing Rick Astley performing "Never Gonna Give You Up".

Expected Response Explanation:

A global search for files with this hash discovers 3 duplicate files:
Jon's iPhone/mobile/Media/DCIM/100APPLE/IMG_0051.MOV
Jon's iPhone/mobile/Media/DCIM/100APPLE/IMG_0052.MOV
Jon's iPhone/mobile/Media/DCIM/100APPLE/IMG_0053.MOV
Viewing the file in a media player shows it as being the music video for Rick Astley's 1987 Hit, Never Gonna Give you Up. This video is commonly used in the online prank known as Rick Rolling, a type of bait and switch using a disguised hyperlink that leads to the music video.

Expected Response Illustration:

Screen Capture from IMG_0053.MOV, Rick Roll

TABLE 1

Question 32

Question 32: What is the address for the stored location in the Google Maps application?

Manufacturer's Expected Response: 21331 Gentry Dr, Sterling, VA 20166

WebCode	Response
232E3H	21331 Gentry Dr, Sterling, VA 20166
23R6RY	21331 Gentry Dr, Sterling, VA 20166
2MP2LK	21331 Gentry Dr, Sterling, VA 20166 This is recovered from the file OnDeviceAliasData under com.google.maps
2U4K6K	16th Street Northwest, Washington, DC
2UJ7EL	Richmond, Richmond, Virginia, United States
2ZD34D	Google Maps not parsed in UFED PA 7.33.0.30. Can't find answer in Google maps plist
3LXYYV	21331 Gentry Dr, Compound building
4KQATB	21331 Gentry Dr, Sterling, VA 20166
4VD9JG	21331 Gentry Dr, Sterling, VA 20166
6LKHCE	21331 Gentry Dr, Sterling, VA 20166
6R89XA	21331 Gentry Dr, Sterling, VA 20166
73ULRR	
7FEZVR	21331 Gentry Dr, Sterling, VA 20166
7NZ8BH	21331 Gentry Dr, Sterling, VA 20166
7TZH7H	21331 Gentry Dr, Sterling, VA 20166
7WXYJC	21331 Gentry Dr, Sterling, VA 20166
82KA7F	Monument avenue richmond
8E9BN8	Cellebrite 7.33.0.30 has not parsed Google Maps
8FY44R	21331 Gentry Dr, Sterling, VA 20166
8XED4T	21331 Gentry Dr, Sterling, VA 20166
93EEZE	21331 Gentry Dr, Sterling, VA 20166
9AEVD6	110 N. Carpenter St., Chicago, IL 60607
9C38CB	21331 Gentry Dr, Sterling, VA 20166
9J3RE7	21331 Gentry Dr, Sterling, VA 20166
A8PRHD	21331 Gentry Dr, Sterling, VA 20166
AB3RE6	singlelineaddress: 21331 Gentry Dr, Sterling, VA 20166, nameandaddress: 21331 Gentry Dr, Sterling, VA 20166, thoroughfare: 21331 Gentry Dr, thoroughfarewithnumber: 21331 Gentry Dr, municipality: Sterling, : Sterling, VA 20166
AJGDN9	21331 Gentry Dr. Sterling, VA 20166

TABLE 1

Question 32	
WebCode	**Response**
AUEEZC	Jon's iPhone/root/Library/Caches/locationd/
B7LJQ6	21331 Gentry Dr, Sterling, VA 20166
BGDYWL	21331 Gentry Dr, Sterling, VA 20166
BK4CEC	21331 Gentry Dr, Sterling, VA 20166
CMVPWM	21331 Gentry Dr, Sterling, VA 20166
CTTKD8	21331 Gentry Dr, Sterling, VA 20166
DDYEJ4	110 N. Carpenter St., Chicago, IL 60607
DGXQF4	21331 Gentry Dr, Sterling, VA 20166
DJL3EA	21331 Gentry Dr, Sterling, VA 20166
EKZT67	21331 Gentry Dr, Sterling, VA 20166
ET7TE8	21331 Gentry Dr, Sterling, VA 20166
FNQKQ8	110 N. Carpenter St., Chicago, IL 60607
FXKMCH	21331 Gentry Dr, Sterling, VA 20166
G3E42G	21331 Gentry Dr, Sterling, VA 20166
GA8EUY	21331 Gentry Dr, Sterling, VA 20166
GJTH2X	21331 Gentry Dr, Sterling, VA 20166
GXBBQ6	21331 Gentry Dr, Sterling, VA 20166
HBTH3W	I-95, Richmond, VA 23227 USA
HRJN96	21331 Gentry Dr, Sterling, VA 20155
JRWEYZ	16th Street Northwest, Washington, DC
KQZJPW	21331 Gentry Dr, Sterling, VA 20166
L2Z97X	I did not locate a stored address in the Google Maps application.
L78WJY	21331 Gentry Dr
LDRZQ3	21331 Gentry Dr, Sterling, VA 20166
LUED6U	21331 Gentry Dr, Sterling, VA 20166
MK4BJT	21331 Gentry Dr, Sterling, VA 20166
P94MFP	None
PBRYEU	21331 Gentry Drive, Sterling, VA 20166
PRFA2W	no address stored in Google Maps application
PVHA3U	21331 Gentry Dr, Sterling, VA 20166
PZYA29	21331 Gentry Dr. Sterling VA 20166

TABLE 1

Question 32	
WebCode	**Response**
Q9J39W	21331 Gentry Dr, Sterling, VA 20166
QBL2JP	21331 Geatry Dr, Sterling, VA 20166
QTQBNV	21331 Gentry Dr, Sterling, VA 20166
QZTKUN	21331 Gentry Drive in Sterling, VA 20166.
RA9UVM	21331 Gentry Dr, Sterling, VA 20166
RWD889	Not Applicable
T6DJYU	21331 Gentry Dr, Sterling, VA 20166
TGQJVM	None Found
TL2WDL	21331 Gentry Dr, Sterling, VA 20166
U2P8ZN	21331 Gentry Dr, Sterling, VA 20166
UCYFWG	21331 Gentry Dr, Sterling, VA 20166
UM9CJR	Black Lives Matter Plaza, Washington DC
UPZBXQ	110 N. Carpenter St., Chicago, IL 60607
UQBAVK	21331 Gentry Dr, Sterling, VA 20166
UTYLUQ	There is no address store in the Google Maps application.
V6M9DQ	Lafayette Square, 16th Street Northwest, Washington, DC.
VJC6V2	21331 Gentry Dr, Sterling, VA 20166
VU246Q	21331 Gentry Dr, Sterling, VA 20166
WJ3TAP	N/A
WX466N	One Apple Park Way, Cupertino, CA 95014 USA
X78WMG	21331 Gentry Dr, Sterling, VA 20166
X8ZRAP	21331 Gentry Drive, Sterling VA, 20166
XJGCUL	21331 Gentry Dr, Sterling, VA 20166
XY9AWG	21331 Gentry Dr, Sterling VA 20166
XYELUY	21331 Gentry Dr, Sterling, VA 20166
YQ9AWF	21331 Gentry Dr, Sterling, VA 20166
Z8D34E	21331 Gentry Dr, Sterling, VA 20166
ZB38DY	21331 Gentry Dr, Sterling, VA 20166
ZX8VNE	(Left blank)

TABLE 1

Question 32

Question 32: What is the address for the stored location in the Google Maps application?

Consensus Result: 21331 Gentry Dr, Sterling, VA 20166

Expected Response Explanation:

Information for the Google Maps application can be found in /mobile/Containers/Data/Application/com.google.Maps/Library/Application Support/OnDeviceAliasData. There is one location stored in this file under "home," 21331 Gentry Dr, Sterling, VA 20166.

Expected Response Illustration:

OnDeviceAliasData

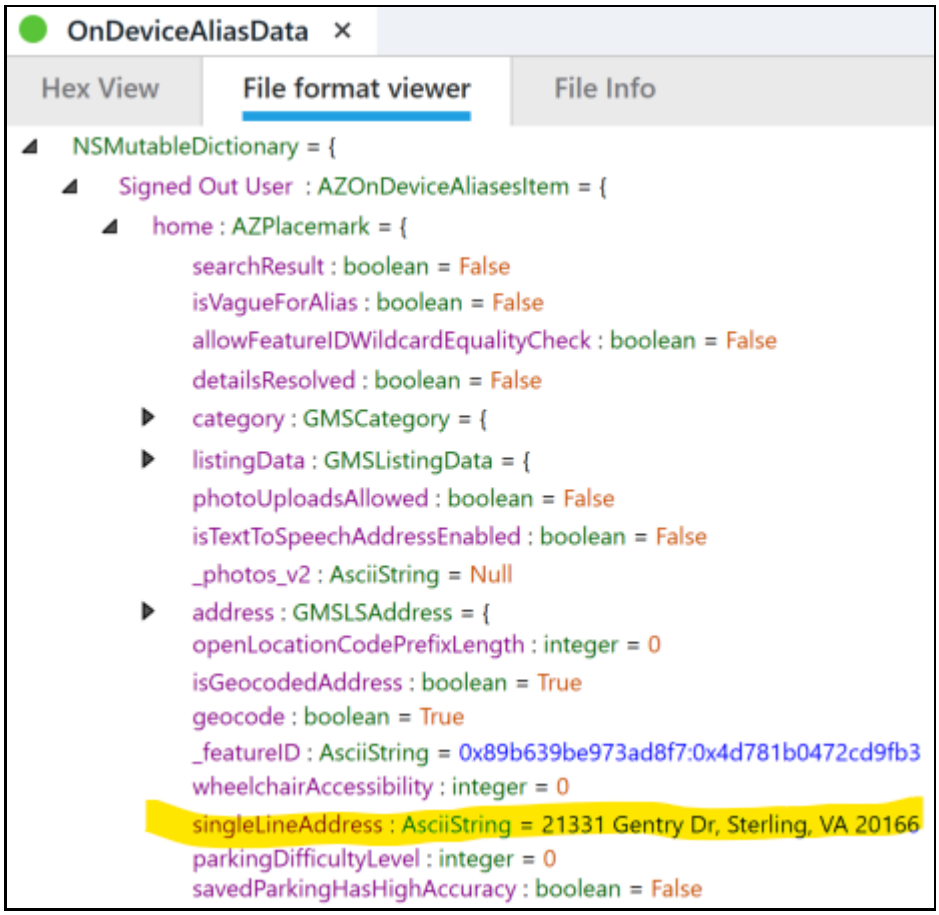


TABLE 1

Question 33

Question 33: What location did the user search in Maps?

Manufacturer's Expected Response: Monument avenue richmond

WebCode	Response
232E3H	Monument avenue richmond
23R6RY	Monument Avenue, Richmond
2MP2LK	Monument avenue richmond
2U4K6K	Monument avenue richmond
2UJ7EL	Monument avenue richmond
2ZD34D	Monument avenue richmond
3LXYYV	Lafayette Square, 16th Street Northwest, Washington, DC
4KQATB	Monument Avenue richmond
4VD9JG	Monument avenue richmond
6LKHCE	Monument avenue richmond
6R89XA	Monument avenue richmond
73ULRR	Monument avenue richmond
7FEZVR	Monument avenue richmond
7NZ8BH	Monument avenue richmond
7TZH7H	Monument avenue richmond
7WXYJC	Monument avenue Richmond
82KA7F	Richmond, Richmond, Virginia, United States
8E9BN8	Monument avenue richmond
8FY44R	Monument avenue richmond
8XED4T	Monument avenue richmond
93EEZE	Richmond, VA
9AEVD6	Monument avenue richmond
9C38CB	Monument avenue richmond
9J3RE7	Monument avenue Richmond
A8PRHD	Monument avenue richmond
AB3RE6	Monument avenue Richmond
AJGDN9	Monument avenue richmond
AUEEZC	Monument avenue richmond
B7LJQ6	Monument avenue richmond

TABLE 1

Question 33	
WebCode	**Response**
BGDYWL	Monument avenue richmond
BK4CEC	Monument Avenue Richmond
CMVPWM	Monument avenue richmond
CTTKD8	Monument avenue richmond
DDYEJ4	Richmond VA
DGXQF4	Richmond, Virginia
DJL3EA	Monument avenue richmond
EKZT67	Monument avenue richmond
ET7TE8	Richmond, Richmond, Virginia, United States
FNQKQ8	Monument avenue richmond
FXKMCH	(37.553029, -77.458578)
G3E42G	Monument avenue richmond
GA8EUY	Richmond, Virginia, United States
GJTH2X	Monument avenue richmond
GXBBQ6	Monument avenue richmond
HBTH3W	Monument avenue richmond
HRJN96	Monument avenue Richmond (37.558086, -77.467195) Richmond, Richmond, Virginia, United States
JRWEYZ	Richmond, Richmond, Virginia, United States
KQZJPW	Richmond, Virginia, United States
L2Z97X	Monument avenue richmond
L78WJY	Monument avenue richmond
LDRZQ3	Monument avenue richmond
LUED6U	Monument avenue richmond
MK4BJT	2395 monument ave, richmond, virginia 23220
P94MFP	Monument avenue richmond
PBRYEU	Our lab does not offer this determination
PRFA2W	Monument avenue richmond
PVHA3U	Monument avenue richmond
PZYA29	Monument avenue richmond
Q9J39W	Monument avenue richmond
QBL2JP	(37.558086, -77.467195)

TABLE 1

Question 33	
WebCode	**Response**
QTQBNV	Monument avenue richmond
QZTKUN	Monument Avenue in Richmond, Virginia
RA9UVM	Richmond, Virginia, United States
RWD889	Monument avenue richmond
T6DJYU	Monument avenue richmond
TGQJVM	Monument avenue richmond
TL2WDL	Monument avenue richmond
U2P8ZN	Monument avenue richmond
UCYFWG	Monument avenue richmond
UM9CJR	Monument avenue richmond
UPZBXQ	Monument avenue richmond
UQBAVK	Monument Avenue
UTYLUQ	Monument Avenue Richmond
V6M9DQ	Monument avenue richmond
VJC6V2	2319 Monument Ave, Richmond VA (37.558086, -77.467195)
VU246Q	Monument avenue richmond
WJ3TAP	Monument avenue richmond
WX466N	Monument avenue richmond
X78WMG	Monument avenue richmond
X8ZRAP	Monument Avenue Richmond
XJGCUL	Monument avenue richmond
XY9AWG	Monument avenue richmond
XYELUY	Monument avenue Richmond
YQ9AWF	Monument avenue richmond
Z8D34E	Monument avenue richmond
ZB38DY	Monument avenue richmond
ZX8VNE	Monument avenue richmond

TABLE 1

Question 33

Question 33: What location did the user search in Maps?

Consensus Result: Monument avenue richmond

Expected Response Explanation:

Data regarding searched places, for the native "Maps" application can be found in mobile/Containers/Data/Application/com.apple.Maps/Library/Maps/GeoHistory.mapsdata.

Expected Response Illustration:

GeoHistory.mapsdata

TABLE 1

Question 34

Question 34: Did the flash fire when taking the photo captured on 6/28/2020 at 12:57:10 PM(UTC-4)? Provide a Yes/No response.

Manufacturer's Expected Response: No

WebCode	Response
232E3H	No
23R6RY	No
2MP2LK	No
2U4K6K	No
2UJ7EL	No
2ZD34D	No. (Flash value = 24 which means auto-flash was on, but did not fire).
3LXYYV	no
4KQATB	No
4VD9JG	No
6LKHCE	No
6R89XA	yes
73ULRR	No
7FEZVR	Yes
7NZ8BH	No
7TZH7H	No
7WXYJC	No
82KA7F	no
8E9BN8	No
8FY44R	No
8XED4T	No
93EEZE	No
9AEVD6	No
9C38CB	No
9J3RE7	No
A8PRHD	No
AB3RE6	NO
AJGDN9	No
AUEEZC	No

TABLE 1

Question 34	
WebCode	**Response**
B7LJQ6	Yes
BGDYWL	No
BK4CEC	No
CMVPWM	No
CTTKD8	No
DDYEJ4	No
DGXQF4	Yes
DJL3EA	No
EKZT67	No
ET7TE8	No
FNQKQ8	No
FXKMCH	No
G3E42G	No
GA8EUY	Yes
GJTH2X	No
GXBBQ6	No
HBTH3W	No
HRJN96	No
JRWEYZ	No
KQZJPW	No
L2Z97X	No
L78WJY	NO
LDRZQ3	No
LUED6U	No
MK4BJT	No
P94MFP	No
PBRYEU	Our lab does not offer this determination
PRFA2W	No
PVHA3U	No
PZYA29	No
Q9J39W	No

TABLE 1

Question 34	
WebCode	**Response**
QBL2JP	No
QTQBNV	No
QZTKUN	No
RA9UVM	No
RWD889	No
T6DJYU	No
TGQJVM	yes
TL2WDL	No
U2P8ZN	No
UCYFWG	No
UM9CJR	No
UPZBXQ	No
UQBAVK	Yes
UTYLUQ	No
V6M9DQ	No
VJC6V2	No
VU246Q	Yes
WJ3TAP	no
WX466N	No
X78WMG	No
X8ZRAP	No
XJGCUL	No
XY9AWG	No
XYELUY	No
YQ9AWF	No
Z8D34E	No
ZB38DY	No
ZX8VNE	No

TABLE 1

Question 34

Question 34: Did the flash fire when taking the photo captured on 6/28/2020 at 12:57:10 PM(UTC-4)? Provide a Yes/No response.

Consensus Result: No

Expected Response Explanation:

Photos taken on an iPhone are stored in /mobile/Media/DCIM/100APPLE. Review of these files for files created on 6/28/2020 at 12:57:10 PM(UTC-4), finds one, IMG_0005.JPG. Review of the EXIF metadata for this file indicates the flash.

Expected Response Illustration:

IMG_0005.JPG EXIF Metadata parsed with 'exiftool v11.88'

```
$ exiftool IMG_0005.JPG
ExifTool Version Number         : 11.88
File Name                       : IMG_0005.JPG
Directory                       : .
File Size                       : 7.0 MB
File Modification Date/Time     : 2020:07:09 23:43:20-04:00
File Access Date/Time           : 2020:11:02 18:13:30-05:00
File Inode Change Date/Time     : 2020:07:09 23:43:20-04:00
File Permissions                : rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone 6s
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 12.3.1
Modify Date                     : 2020:06:28 12:57:10
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/1374
F Number                        : 2.2
Exposure Program                : Program AE
ISO                             : 25
Exif Version                    : 0221
Date/Time Original              : 2020:06:28 12:57:10
Create Date                     : 2020:06:28 12:57:10
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/1374
Aperture Value                  : 2.2
Brightness Value                : 10.48891732
Exposure Compensation           : 0
Metering Mode                   : Multi-segment
Flash                           : Auto, Did not fire
Focal Length                    : 4.2 mm
```

TABLE 1

Question 35

Question 35: When did the user LAST visit news.google.com in the Safari browser? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset).

Manufacturer's Expected Response: 07/05/2020 01:07 PM (UTC-4)

WebCode	Response
232E3H	07/05/2020 01:07 PM (UTC-4)
23R6RY	07/05/2020 01:07 PM (UTC-4)
2MP2LK	7/5/2020 13:07(UTC-4)
2U4K6K	05/07/2020 1:07 PM (UTC-4)
2UJ7EL	07/05/2020 01:07:12 PM(UTC -4)
2ZD34D	07/05/2020 13:04:36pm(UTC-4)
3LXYYV	07/05/2020 12:04 PM (UTC -5)
4KQATB	07/05/2020 13:07
4VD9JG	07/05/2020 01:07 PM (UTC-4)
6LKHCE	07/25/2020 01:07 PM (UTC-4)
6R89XA	07.05.2020 01:07:12(UTC-4) pm
73ULRR	07/05/2020 01:07 PM (UTC-4)
7FEZVR	07/05/2020 01:07 PM (UTC-4)
7NZ8BH	07/05/2020 01:07 PM (UTC-4)
7TZH7H	07/05/2020 01:07 PM (UTC-4)
7WXYJC	07/05/2020 01:07 PM
82KA7F	07/05/2020 05:07 pm (UTC+0)
8E9BN8	07/05/2020 13:07:12 PM (UTC-4)
8FY44R	7/5/2020 1:07:12 PM(UTC-4)
8XED4T	7/5/2020 1:07:12 PM(UTC-4)
93EEZE	07/05/2020 01:07 PM(UTC-4)
9AEVD6	07/05/2020, 01:07:12 (UTC-4)
9C38CB	07/05/2020 01:07 PM (UTC-4)
9J3RE7	07/05/2020 13:07 PM (UTC-4)
A8PRHD	07/05/2020 13:07 PM (UTC-4)
AB3RE6	07/05/2020 01:07 PM (UTC-4)
AJGDN9	07/05/2020 01:07 PM (UTC -4)
AUEEZC	07/05/2020 01:07 PM (UTC-4)

TABLE 1

Question 35	
WebCode	**Response**
B7LJQ6	07/05/2020 13:07 PM
BGDYWL	07/05/2020 01:07 PM (UTC-4)
BK4CEC	07/05/2020 01:07 PM (UTC-4)
CMVPWM	07/05/2020 01:07 PM (UTC-4)
CTTKD8	07/05/2020 01:07 PM (UTC-4)
DDYEJ4	07/05/2020 1:07 PM (UTC-4)
DGXQF4	07/05/2020 01:07 PM(UTC-4)
DJL3EA	7/5/2020 1:07 PM(UTC-4)
EKZT67	06/27/2020 12:54 PM (UTC-4)
ET7TE8	07/05/2020 13:07(UTC-4) PM
FNQKQ8	07/05/2020 01:07:12 PM (0x4EC5)
FXKMCH	07/05/2020 01:07 PM (UTC-4)
G3E42G	7/5/2020 1:07:12 PM(UTC-4)
GA8EUY	07/05/2020 13:04:36 PM (UTC-4)
GJTH2X	7/5/2020 1:07 PM(UTC-4)
GXBBQ6	07/05/2020 01:07 PM (UTC-4)
HBTH3W	07/05/2020 01:07 PM (UTC-4)
HRJN96	07/05/2020 12:04(UTC-5)
JRWEYZ	07/05/2020 01:04 PM (UTC-4)
KQZJPW	07/05/2020 01:04 PM (UTC-4), however on 07/05/2020 1:07 PM (UTC-4) a visit to a sub-page within news.google.com was made
L2Z97X	7/5/2020 13:07(UTC-4)
L78WJY	07/05/2020 01:07PM (UTC-4)
LDRZQ3	07/05/2020 01:07 PM (UTC-4)
LUED6U	07/05/2020 01:07 PM (UTC-4)
MK4BJT	07/05/2020 01:07 PM (UTC-4)
P94MFP	7/5/2020 1:07:12 PM(UTC-4)
PBRYEU	https://news.google.com 07/05/2020 01:04 PM (UTC -4:00) https://news.google.com/topstories?hl=en-us&gl=us&ceid=us:en 07/05/2020 01:07 PM (UTC -4:00)
PRFA2W	07/05/2020 13:07 PM
PVHA3U	7/05/2020 1:07:12 PM(UTC-4)
PZYA29	07/05/2020 01:07 PM(UTC-4)

TABLE 1

Question 35	
WebCode	**Response**
Q9J39W	07/05/2020 01:07 PM (UTC-4)
QBL2JP	07/05/2020 01:07 PM (UTC-4)
QTQBNV	7/5/2020 13:04(UTC-4) (See note in comments) [Table 2 - Additional Comments]
QZTKUN	07/05/2020 at 01:07 PM (UTC-4)
RA9UVM	07/05/2020 12:07 PM offset 0x4EC5
RWD889	07/05/2020 1:07:12 PM (UTC-4)
T6DJYU	07/05/2020 01:07 PM (UTC-4)
TGQJVM	7/5/2020 10:07:12 AM (UTC-7)
TL2WDL	07/05/2020 1:07 PM (UTC-4)
U2P8ZN	07/05/2020 01:07 PM (UTC-4)
UCYFWG	7/5/2020 1:07 PM(UTC-4)
UM9CJR	7/5/2020 1:07:12 PM (UTC-4)
UPZBXQ	07/05/2020 01:07 PM(UTC-4)
UQBAVK	07/05/2020 12:07 (UTC-5)
UTYLUQ	07/05/2020 01:07 PM (UTC -4)
V6M9DQ	7/5/2020 1:07 PM (UTC-4)
VJC6V2	07/05/2020 5:07:12 PM
VU246Q	07/5/2020 01:04 (UTC-4)
WJ3TAP	7/5/2020 1:04:38 PM(UTC-4)
WX466N	07/05/2020 1:07 PM (UTC-4)
X78WMG	07/05/2020 01:07(UTC-4) PM
X8ZRAP	07/05/2020 01:12 PM (UTC-4)
XJGCUL	07/05/2020 01:07 PM (UTC-4)
XY9AWG	7/5/2020 1:07 PM (UTC -4)
XYELUY	7/5/2020 1:07:12 PM (UTC-4)
YQ9AWF	07/05/2020 13:07PM (UTC -4) or 1:07PM(UTC -4)
Z8D34E	7/5/2020 1:07 PM(UTC-4)
ZB38DY	7/5/2020 1:07:12 PM(UTC-4)
ZX8VNE	07/05/2020 13:04 AM (UTC-4)

TABLE 1

Question 35

Question 35: When did the user LAST visit news.google.com in the Safari browser? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset).

Consensus Result: 07/05/2020 01:07 PM (UTC-4) and all formatting styles to include other time zones which represent the same information. In addition, due to the ambiguity of the question, the same date with the time of 01:04 PM was also accepted.

Expected Response Explanation:

Safari browser history is stored in /mobile/Library/Safari/History.db. Review of the records in this database show the last visit to news.google.com occurred 7/5/2020 1:07:12 PM(UTC-4).

Expected Response Illustration:

Database View of Safari/History.db (*UTC TIME)

History.db

File Info

history_visits (9)

id	history_it	visit_time	title	load_successful
9	5	7/5/2020 5:07:36 PM	Top 30 Funny Animal Memes Of The Week	1
8	4	7/5/2020 5:07:14 PM	Dump a Day - There's Nothing Quite Like a Good Dump - Dump A Day	1
7	3	7/5/2020 5:07:12 PM	Google News	1
6	4	7/5/2020 5:06:52 PM	Dump a Day - There's Nothing Quite Like a Good Dump - Dump A Day	1
5	1	7/5/2020 5:04:36 PM		1
4	3	7/5/2020 5:04:36 PM	Google News	1
3	3	7/5/2020 5:04:38 PM	Google News	1
2	2	7/4/2020 6:58:58 PM	Activate Your App | McDonald's	1
1	1	6/27/2020 4:54:49 PM	Cannot Open Page	0

Cellebrite "Web History" table showing last visit to Google News

Web History (72) | History.db

Last Visited	Title	Source	URL	Visits
7/5/2020 8:50:40 PM(UTC-4)	rsalcau.com/bdv_rd.dbm?enparms2=1775%...	Chrome	http://rsalcau.com/bdv_rd.dbm?enparms2=1775%2C1908023%2C28...	
7/5/2020 1:07:36 PM(UTC-4)	Top 30 Funny Animal Memes Of The Week	Safari	http://www.dumpaday.com/funny-animals/top-30-funny-animal-me...	1
7/5/2020 1:07:14 PM(UTC-4)	Dump a Day - There's Nothing Quite Like a...	Safari	http://www.dumpaday.com/	1
7/5/2020 1:07:12 PM(UTC-4)	Google News	Safari	https://news.google.com/topstories?hl=en-US&gl=US&ceid=US:en	1
7/5/2020 1:06:52 PM(UTC-4)	Dump a Day - There's Nothing Quite Like a...	Safari	http://www.dumpaday.com/	1
7/5/2020 1:04:38 PM(UTC-4)	Google News	Safari	https://news.google.com/topstories?hl=en-US&gl=US&ceid=US:en	1
7/5/2020 1:04:36 PM(UTC-4)		Safari	http://news.google.com/	1
7/5/2020 1:04:36 PM(UTC-4)	Google News	Safari	https://news.google.com/topstories?hl=en-US&gl=US&ceid=US:en	1

TABLE 1

Question 36

Question 36: What type of payment card website did the user visit in the Chrome browser?

Manufacturer's Expected Response: Prepaid reloadable debit, Vanilla, or My Vanilla

WebCode	Response
232E3H	MyVanilla Card
23R6RY	MyVanilla Reloadable Prepaid Card
2MP2LK	MyVanilla Reloadable Prepaid Card
2U4K6K	MyVanilla Reloadable Prepaid Card
2UJ7EL	MyVanilla Reloadable Prepaid Card
2ZD34D	http://myvanilladebitcard.com/
3LXYYV	https://www.myvanillacard.com
4KQATB	MyVanilla Reloadable Prepaid Card
4VD9JG	Reloadable Prepaid Card
6LKHCE	MyVanilla Reloadable Prepaid Card (URL http://myvanilladebitcard.com/)
6R89XA	MyVanilla Reloadable Prepaid Card
73ULRR	MyVanilla Reloadable Prepaid Card
7FEZVR	MyVanilla Reloadable Prepaid Card
7NZ8BH	MyVanilla Reloadable Prepaid Card
7TZH7H	MyVanilla Reloadable Prepaid Card (https://www.myvanillacard.com)
7WXYJC	MyVanilla
82KA7F	http://myvanilladebitcard.com/ MyVanilla Reloadable Prepaid Card
8E9BN8	Reloadable Prepaid Card
8FY44R	MyVanilla Reloadable Prepaid Card
8XED4T	MyVanilla Reloadable Prepaid Card
93EEZE	MyVanilla Reloadable Prepaid Card
9AEVD6	https://www.myvanillacard.com and http://myvanilladebitcard.com/
9C38CB	MyVanilla Reloadable Prepaid Card
9J3RE7	MyVanilla Reloadable Prepaid Card
A8PRHD	Vanilla Card
AB3RE6	Reloadable Prepaid card
AJGDN9	MyVanilla Reloadable Prepaid Card
AUEEZC	Debit Card
B7LJQ6	Debit Card - http://myvanilladeditcard.com/

TABLE 1

Question 36	
WebCode	**Response**
BGDYWL	MyVanilla Reloadable Prepaid Card
BK4CEC	MyVanilla Reloadable Prepaid Card
CMVPWM	Vanilla Reloadable Prepaid Card
CTTKD8	reloadable prepaid card
DDYEJ4	MyVanilla debit card
DGXQF4	MyVanilla Reloadable Prepaid Card
DJL3EA	MyVanilla Reloadable Prepaid Card
EKZT67	Reloadable Prepaid Card
ET7TE8	https://www.myvanillacard.com http://myvanilladebitcard.com
FNQKQ8	MyVanilla Reloadable Prepaid Card
FXKMCH	MyVanilla Reloadable Prepaid Card website
G3E42G	MyVanilla Reloadable Prepaid Card
GA8EUY	MyVanilla Reloadable Prepaid Card
GJTH2X	Vanilla Reloadable Prepaid Card
GXBBQ6	MyVanilla Reloadable Prepaid Card
HBTH3W	Reloadable Prepaid Card (MyVanilla)
HRJN96	MyVanilla Reloadable Prepaid Card
JRWEYZ	MyVanilla Reloadable Prepaid card
KQZJPW	myvanillacard.com
L2Z97X	MyVanilla Reloadable Prepaid Card
L78WJY	MyVanilla Reloadable Prepaid Card
LDRZQ3	MyVanilla Reloadable Prepaid Card
LUED6U	www.myvanillacard.com, a reloadable prepaid card website.
MK4BJT	Prepaid Card
P94MFP	Prepaid card
PBRYEU	myvanilladebitcard.com MyVanilla Reloadable Prepaid Card
PRFA2W	Reloadable Prepaid Card
PVHA3U	A reloadable prepaid card website.
PZYA29	MyVanilla Reloadable Prepaid Card
Q9J39W	MyVanilla Reloadable Prepaid Card
QBL2JP	https://www.myvanillacard.com

TABLE 1

Question 36	
WebCode	**Response**
QTQBNV	MyVanilla Reloadable Prepaid Card (https://www.myvanillacard.com/)
QZTKUN	MyVanilla Reloadable Prepaid card
RA9UVM	My Vanilla Card (Prepaid Card)
RWD889	MyVanilla Reloadable Prepaid Card
T6DJYU	MyVanilla Reloadable Prepaid Card
TGQJVM	MyVanilla Reloadable Prepaid Card
TL2WDL	Vanilla
U2P8ZN	MyVanilla Reloadable Prepaid Card
UCYFWG	http://myvanilladebitcard.com
UM9CJR	MyVanilla Reloadable Prepaid Card
UPZBXQ	MyVanilla Reloadable Prepaid Card
UQBAVK	http://myvanilladebitcard.com/MyVanilla Reloadable Prepaid Card http://myvanilladebitcard.com/
UTYLUQ	Vanilla Re-loadable Prepaid Card
V6M9DQ	MyVanilla Reloadable Prepaid Card (https://www.myvanillacard.com/)
VJC6V2	www.myvanillacard.com
VU246Q	e-token
WJ3TAP	MyVanilla Reloadable Prepaid Card
WX466N	MyVanilla Reloadable Prepaid Card
X78WMG	MyVanilla Reloadable Prepaid Card
X8ZRAP	My Vanilla Reloadable prepaid card
XJGCUL	Vanilla
XY9AWG	MyVanilla
XYELUY	MyVanilla Reloadable Prepaid Card
YQ9AWF	MyVanilla Reloadable Prepaid Card
Z8D34E	Vanilla
ZB38DY	MyVanilla Reloadable Prepaid Card www.myvanillacard.com
ZX8VNE	A reloadable prepaid card from the myVanillacard.com website

TABLE 1

Question 36

Question 36: What type of payment card website did the user visit in the Chrome browser?

Consensus Result: Prepaid reloadable debit, Vanilla, or My Vanilla and all formatting styles which represent the same information.

Expected Response Explanation:

Chrome browser history is stored in /mobile/Containers/Data/Application/com.google.chrome.ios/Library/Application Support/Google/Chrome/Default/History. Review of the records in this database show visits to www.myvanillacard.com on July 5, 2020.

Expected Response Illustration:

Database View of Chrome History showing visits to myvanillacard.com

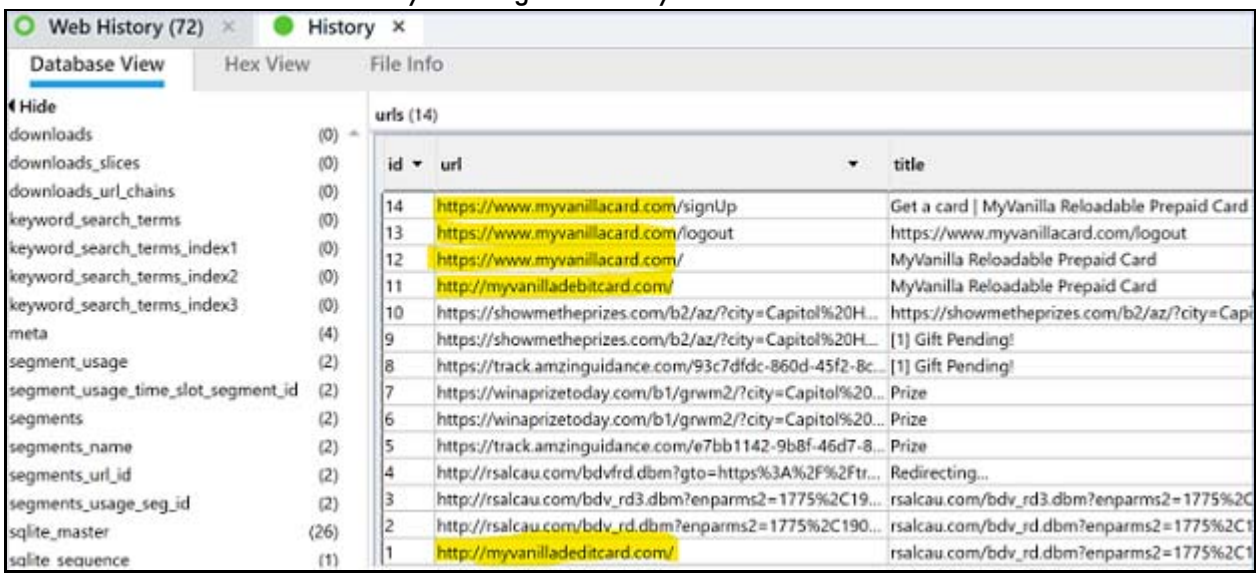


TABLE 1

Question 37

Question 37: What did the user create a reminder to do?

Manufacturer's Expected Response: Backup phone

WebCode	Response
232E3H	Backup phone
23R6RY	Backup phone
2MP2LK	Backup phone
2U4K6K	Backup phone
2UJ7EL	Backup phone
2ZD34D	Backup phone
3LXYYV	Backup phone
4KQATB	Backup phone
4VD9JG	Backup phone
6LKHCE	Backup phone
6R89XA	Backup phone
73ULRR	Backup phone
7FEZVR	Backup phone
7NZ8BH	Backup phone
7TZH7H	Backup phone
7WXYJC	Backup phone
82KA7F	Backup phone
8E9BN8	Backup phone
8FY44R	Backup phone
8XED4T	Backup phone
93EEZE	Backup phone
9AEVD6	Backup phone
9C38CB	Backup phone
9J3RE7	Backup phone
A8PRHD	Backup phone
AB3RE6	Backup phone
AJGDN9	Backup Phone
AUEEZC	Backup phone
B7LJQ6	Backup phone

TABLE 1

Question 37	
WebCode	**Response**
BGDYWL	Backup phone
BK4CEC	Backup phone
CMVPWM	Backup phone
CTTKD8	Backup phone
DDYEJ4	Backup phone
DGXQF4	Backup phone
DJL3EA	Backup phone
EKZT67	Backup phone
ET7TE8	Backup phone
FNQKQ8	Backup phone
FXKMCH	Backup phone
G3E42G	Backup phone
GA8EUY	Backup phone
GJTH2X	Backup phone
GXBBQ6	Backup phone
HBTH3W	Backup phone
HRJN96	Backup phone
JRWEYZ	Backup phone
KQZJPW	Backup phone
L2Z97X	Backup phone
L78WJY	Backup Phone
LDRZQ3	Backup phone
LUED6U	Backup phone
MK4BJT	Backup phone
P94MFP	Backup phone
PBRYEU	Backup phone
PRFA2W	Backup phone
PVHA3U	Backup phone
PZYA29	backup phone
Q9J39W	Backup phone
QBL2JP	Backup phone

TABLE 1

Question 37	
WebCode	**Response**
QTQBNV	Backup phone
QZTKUN	Backup phone
RA9UVM	Backup phone
RWD889	Visit dc
T6DJYU	Backup phone
TGQJVM	Backup Phone
TL2WDL	Backup phone
U2P8ZN	Backup phone
UCYFWG	Backup phone
UM9CJR	Backup phone
UPZBXQ	Backup phone
UQBAVK	Backup phone
UTYLUQ	Back-up iPhone
V6M9DQ	Backup phone
VJC6V2	Backup Phone
VU246Q	Backup phone
WJ3TAP	Backup phone
WX466N	Backup phone
X78WMG	Backup phone
X8ZRAP	backup phone
XJGCUL	Backup phone
XY9AWG	Backup phone
XYELUY	Backup phone
YQ9AWF	Backup Phone
Z8D34E	Backup Phone
ZB38DY	Backup phone
ZX8VNE	back up phone

TABLE 1

Question 37

Question 37: What did the user create a reminder to do?

Consensus Result: Backup phone

Expected Response Explanation:

iPhone reminders are stored in /mobile/Library/Reminders/. Only one reminder with content was on this device.

Expected Response Illustration:

Cellebrite "Calendar" view showing Reminder to Backup phone

Subject	Category	Account	Source		Source file information
Backup phone	Reminders		Reminders		Data-38D4E87A-350D-4ADE-B0CF-7FD2BE5FC04B.sqlite : 0x3753C

TABLE 1

Question 38

Question 38: When was the user scheduled to end his visit to DC? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset).

Manufacturer's Expected Response: 07/03/2020 07:59 PM(UTC-4)

WebCode	Response
232E3H	07/03/2020 07:59 PM (UTC-4)
23R6RY	07/03/2020 07:59 PM (UTC-4)
2MP2LK	7/3/2020 19:59(UTC-4)
2U4K6K	03/07/2020 7:59 (UTC-4)
2UJ7EL	07/03/2020 07:59:59 PM(UTC -4)
2ZD34D	07/03/2020 19:59:59pm(UTC-4)
3LXYYV	07/03/2020 18:59 PM (UTC-5)
4KQATB	07/03/2020 19:59 PM
4VD9JG	07/03/2020 7:59 PM (UTC-4)
6LKHCE	07/03/2020 07:59 PM (UTC-4)
6R89XA	07.03.2020 07:59:59(UTC-4) pm
73ULRR	07/03/2020 07:59 PM (UTC-4)
7FEZVR	07/03/2020 07:59 PM (UTC-4)
7NZ8BH	07/03/2020 07:59 PM (UTC-4)
7TZH7H	07/03/2020 07:59 PM (UTC-4)
7WXYJC	07/03/2020 07:59 PM
82KA7F	07/03/2020 11:59 PM (UTC+0)
8E9BN8	07/03/2020 19:59:59 PM (UTC-4)
8FY44R	7/3/2020 7:59:59 PM(UTC-4)
8XED4T	7/3/2020 7:59:59 PM(UTC-4)
93EEZE	07/03/2020 07:59 PM(UTC-4)
9AEVD6	07/03/2020, 07:59:59PM (UTC-4)
9C38CB	07/03/2020 07:59 PM (UTC-4)
9J3RE7	07/03/2020 19:59 PM (UTC-4)
A8PRHD	07/032/2020 19:59 PM (UTC-4)
AB3RE6	07/03/2020 07:59 PM (UTC-4)
AJGDN9	07/03/2020 07:59 PM (UTC -4)
AUEEZC	07/03/2020 07:59 PM (UTC-4)

TABLE 1

Question 38	
WebCode	**Response**
B7LJQ6	07/03/2020 19:59 PM
BGDYWL	07/03/2020 07:59 PM (UTC-4)
BK4CEC	07/03/2020 07:59 PM (UTC-4)
CMVPWM	07/03/2020 07:59 PM (UTC-4)
CTTKD8	07/03/2020 07:59 PM (UTC-4)
DDYEJ4	07/03/2020 07:59 PM (UTC-4)
DGXQF4	07/03/2020 7:59 PM(UTC-4)
DJL3EA	7/3/2020 7:59 PM(UTC-4)
EKZT67	07/03/2020 07:59 PM (UTC-4)
ET7TE8	07/03/2020 19:59 PM(UTC-4)
FNQKQ8	07/03/2020 07:59:59 PM (0x94A96)
FXKMCH	07/03/2020 7:59 PM (UTC-4)
G3E42G	7/3/2020 7:59:59 PM(UTC-4)
GA8EUY	07/03/2020 19:59:59 PM (UTC-4)
GJTH2X	7/3/2020 7:59 PM (UTC-4)
GXBBQ6	07/03/2020 07:59 PM (UTC-4)
HBTH3W	07/03/2020 01:07 PM (UTC-4)
HRJN96	07/03/2020 18:59(UTC-5)
JRWEYZ	07/03/2020 07:59 PM (UTC-4)
KQZJPW	07/03/2020 07:59 PM (UTC-4)
L2Z97X	7/3/2020 19:59(UTC-4)
L78WJY	07/03/2020 07:59PM (UTC-4)
LDRZQ3	07/03/2020 07:59 PM (UTC-4)
LUED6U	07/03/2020 07:59 PM (UTC-4)
MK4BJT	07/03/2020 07:59 p.m. (UTC -4)
P94MFP	7/3/2020 7:59:59 PM(UTC-4)
PBRYEU	07/03/2020 7:59 PM (UTC -4:00)
PRFA2W	07/03/2020 19:59 PM
PVHA3U	7/3/2020 7:59:59 PM(UTC-4)
PZYA29	07/03/2020 07:59 PM(UTC-4)
Q9J39W	07/03/2020 07:59 PM (UTC-4)

TABLE 1

Question 38	
WebCode	**Response**
QBL2JP	07/03/2020 07:59 PM (UTC-4)
QTQBNV	7/3/2020 19:59(UTC-4)
QZTKUN	07/03/2020 at 07:59 PM (UTC-4)
RA9UVM	07/03/2020 6:59 PM (UTC -5) offset 0x94A8C
RWD889	07/03/2020 7:59:59 PM (UTC-4)
T6DJYU	07/03/2020 07:59 PM (UTC-4)
TGQJVM	7/3/2020 4:59:59 PM (UTC-7)
TL2WDL	07/03/2020 7:59 PM (UTC-4)
U2P8ZN	07/03/2020 07:59 PM (UTC-4)
UCYFWG	07/03/2020 7:59 PM(UTC-4)
UM9CJR	7/3/2020 7:59:59 PM(UTC-4)
UPZBXQ	07/03/2020 07:59 PM(UTC-4)
UQBAVK	07/04/2020 13:40 PM (UTC-5)
UTYLUQ	This information is unknown.
V6M9DQ	7/3/2020 7:59 PM (UTC-4)
VJC6V2	7/3/2020 7:59:59 PM(UTC-4
VU246Q	07/3/2020 07:59 PM (UTC-4)
WJ3TAP	7/3/2020 7:59:59 PM(UTC-4)
WX466N	07/03/2020 7:59 PM (UTC-4)
X78WMG	07/03/2020 07:59(UTC-4) PM
X8ZRAP	07/03/2020 07:59 PM (UTC-4)
XJGCUL	07/03/2020 07:59 PM (UTC-4)
XY9AWG	7/3/2020 7:59 pm (UTC -4)
XYELUY	7/3/2020 7:59:59 PM (UTC-4)
YQ9AWF	07/09/2020 7:59PM(UTC -4) or 19:59PM(UTC-4)
Z8D34E	7/3/2020 7:59 PM(UTC-4)
ZB38DY	7/3/2020 7:59:59 PM(UTC-4)
ZX8VNE	07/03/2020 07:59 PM (UTC-4)

TABLE 1

Question 38

Question 38: When was the user scheduled to end his visit to DC? Provide the answer in the time zone set for the device using the following format: MM/DD/YYYY HH:MM AM/PM (Offset).

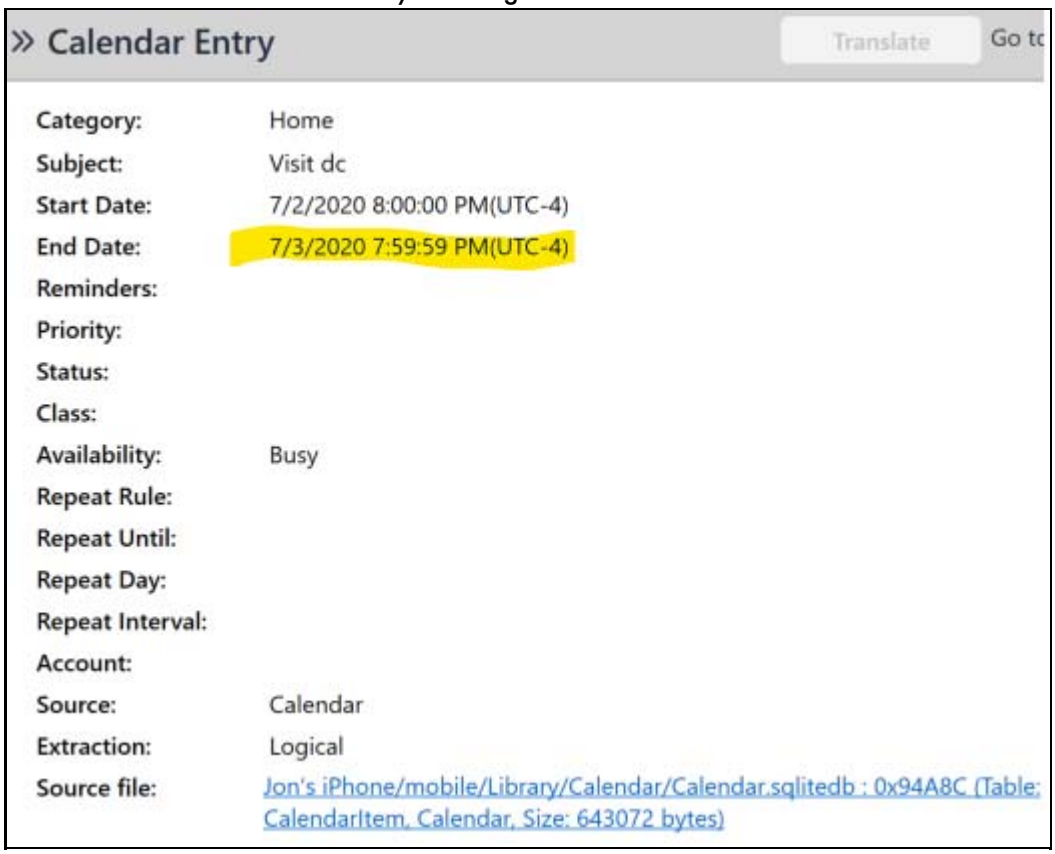
Consensus Result: 07/03/2020 07:59 PM(UTC-4) and all formatting styles to include different time zones which represent the same information.

Expected Response Explanation:

Calendar entries are stored in /mobile/Library/Calendar/Calendar.sqlitedb. The entry for "Visit dc" was scheduled from 7/2/2020 8:00:00 PM(UTC-4) to 7/3/2020 7:59:59 PM(UTC-4).

Expected Response Illustration:

Cellebrite view of Calendar entry showing start and end dates



Database view of Calendar.sqlitedb showing end date for "Visit dc" entry

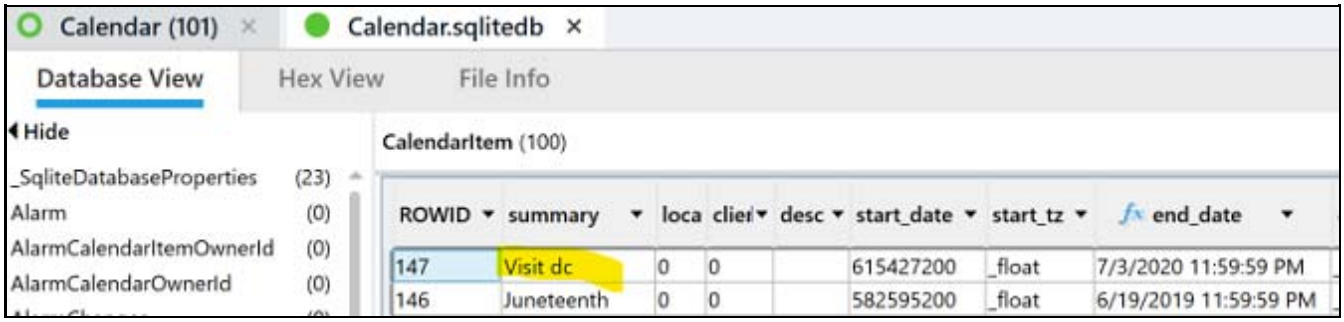


TABLE 1

Question 39

Question 39: What are the location coordinates of the device on 6/28/2020 at 12:51:59 PM (UTC-4)? Provide your response using the following format: Latitude, Longitude.

Manufacturer's Expected Response: 37.558086, -77.467195

WebCode	Response
232E3H	37.5580867, -77.4671943
23R6RY	37.558086, -77.467195
2MP2LK	(37.558086, -77.467195)
2U4K6K	37.558086, -77.467195
2UJ7EL	(35.558086, -77.467195)
2ZD34D	(37.558086, -77.467195)
3LXYYV	(37.558400, -77.467600)
4KQATB	37.558086, -77.467195
4VD9JG	37.558086, -77.467195
6LKHCE	37.558086, -77.467195
6R89XA	(37.558086, -77.467195)
73ULRR	37.558086, -77.467195
7FEZVR	37.558086, -77.467195
7NZ8BH	37.558086, -77.467195
7TZH7H	37.558086, -77.467195
7WXYJC	37.558086, -77.467195
82KA7F	(37.558086, -77.467195)
8E9BN8	37.558086, -77.467195
8FY44R	(37.558086, -77.467195)
8XED4T	(37.558086, -77.467195)
93EEZE	(37.558086, -77.467195)
9AEVD6	(37.558086, -77.467195)
9C38CB	37.558086, -77.467195
9J3RE7	37.558086, -77.467195
A8PRHD	37.558086, -77.467195
AB3RE6	37.558086, -77.467195
AJGDN9	37.558086, -77.467195
AUEEZC	37.558086, -77.467195

TABLE 1

Question 39	
WebCode	**Response**
B7LJQ6	(37.558086, -77.467195)
BGDYWL	37.558086, -77.467195
BK4CEC	37.558086, -77.467195
CMVPWM	37.558086, -77.467195
CTTKD8	37.558086, -77.467195
DDYEJ4	(37.558086, -77.467195)
DGXQF4	37.558086, -77.467195
DJL3EA	37.558086, -77.467195
EKZT67	37.558086, -77.467195
ET7TE8	37.558086, -77.467195
FNQKQ8	37.5580867, -77.4671943
FXKMCH	37.558086, -77.467195
G3E42G	37.558086, -77.467195
GA8EUY	(37.558086, -77.467195)
GJTH2X	(37.558086, -77.467195)
GXBBQ6	-77.467195, 37.558086
HBTH3W	(37.558086, -77.467195)
HRJN96	(37.558086, -77.467159)
JRWEYZ	37.558086, -77.467195
KQZJPW	(37.558086, -77.467195)
L2Z97X	(37.558086, -77.467195)
L78WJY	37.558086, -77.467195
LDRZQ3	37.558086, -77.467195
LUED6U	37.558086, -77.467195 Additionally, GeoHistory.mapsdata display's the coordinates 37.5580867, -77.4671943
MK4BJT	37.558086, -77.467195
P94MFP	37.558086, -77.467195
PBRYEU	37.558086, -77.467195
PRFA2W	37.558086 -77.467195
PVHA3U	37.558086, -77.467195
PZYA29	37.558086, -77.467195
Q9J39W	37.558086, -77.467195

TABLE 1

Question 39	
WebCode	**Response**
QBL2JP	(37.558086, -77.467195)
QTQBNV	(37.558086, -77.467195)
QZTKUN	37.558086,-77.467195
RA9UVM	Latitude: 37.5584916666667 Longitude:-77.467505
RWD889	(37.558086, -77.467195)
T6DJYU	37.558086, -77.467195
TGQJVM	37.558500, -77.467500
TL2WDL	37.558086, -77.467195
U2P8ZN	37.558086, -77.467195
UCYFWG	37.558086, -77.467195
UM9CJR	37.558086, -77.467195
UPZBXQ	37.558086, -77.467195
UQBAVK	(37.558086, -77.467195)
UTYLUQ	(37.558086, -77.467195)
V6M9DQ	37.558086, -77.467195
VJC6V2	(37.558086, -77.467195)
VU246Q	37.558086, -77.467195
WJ3TAP	37.558086, -77.467195
WX466N	37.558086, -77.467195
X78WMG	37.558086, -77.467195
X8ZRAP	37.558086, -77.467195
XJGCUL	37.5580867, -77.4671943
XY9AWG	(37.558086, -77.467195)
XYELUY	(37.558086, -77.467195)
YQ9AWF	37.558086, -77.468003
Z8D34E	(37.558086, -77.467195)
ZB38DY	(37.558086, -77.467195)
ZX8VNE	37.558086, -77.467195

TABLE 1

Question 39

Question 39: What are the location coordinates of the device on 6/28/2020 at 12:51:59 PM (UTC-4)? Provide your response using the following format: Latitude, Longitude.

Consensus Result: 37.558086, -77.467195

Expected Response Explanation:

The Cellebrite Device Locations pane aggregates location data from many sources and places the entries in a table for easy sorting and review. In this case, a record for a GPS fix was extracted from /mobile/Containers/Data/Application/com.apple.Maps/Library/Maps/GeoHistory.mapsdata.

Expected Response Illustration:

Cellebrite "Device Locations" view showing GPS fix on 6/28/2020 at 12:51:59 PM (UTC-4)

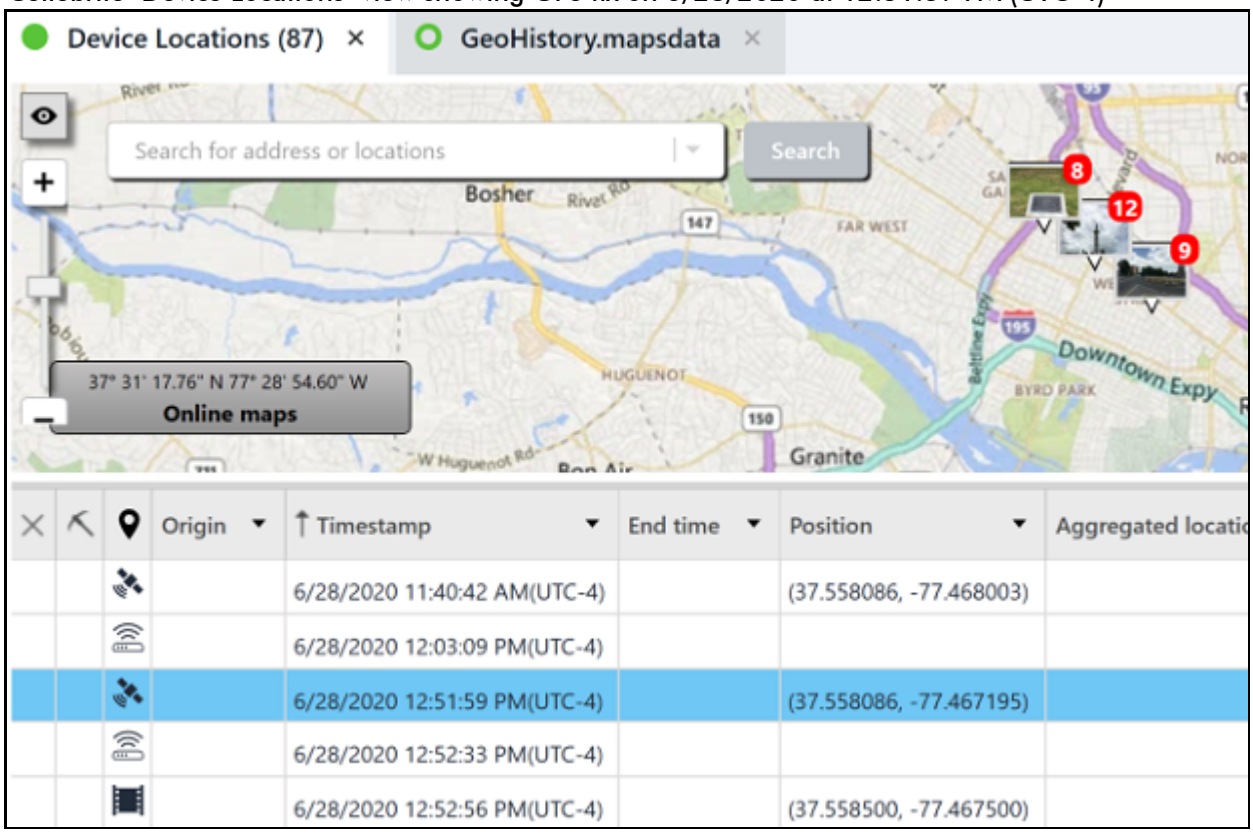


TABLE 1

Question 40

Question 40: Provide the content of a note created with the notes app.

Manufacturer's Expected Response: Something noteworthy

WebCode	Response
232E3H	Something noteworthy
23R6RY	Something noteworthy
2MP2LK	Something noteworthy
2U4K6K	Something noteworthy
2UJ7EL	Something noteworthy
2ZD34D	Something noteworthy
3LXYYV	Something noteworthy
4KQATB	Something noteworthy
4VD9JG	Something noteworthy
6LKHCE	Something noteworthy
6R89XA	Something noteworthy
73ULRR	Something noteworthy
7FEZVR	Something noteworthy
7NZ8BH	Something noteworthy
7TZH7H	Something noteworthy
7WXYJC	Something noteworthy
82KA7F	Something noteworthy
8E9BN8	Something noteworthy
8FY44R	Something noteworthy
8XED4T	Something noteworthy
93EEZE	Something noteworthy
9AEVD6	Something noteworthy
9C38CB	Something noteworthy
9J3RE7	Something noteworthy
A8PRHD	Something noteworthy
AB3RE6	Something noteworthy
AJGDN9	Something noteworthy
AUEEZC	Something noteworthy
B7LJQ6	Something noteworthy

TABLE 1

Question 40	
WebCode	**Response**
BGDYWL	Something noteworthy
BK4CEC	« Something noteworthy »
CMVPWM	Something noteworthy
CTTKD8	Something noteworthy
DDYEJ4	Something noteworthy
DGXQF4	Something noteworthy
DJL3EA	Something noteworthy
EKZT67	Something noteworthy
ET7TE8	Something noteworthy
FNQKQ8	Something noteworthy
FXKMCH	Something noteworthy
G3E42G	Something noteworthy
GA8EUY	Something noteworthy
GJTH2X	Something noteworthy
GXBBQ6	Something noteworthy
HBTH3W	Something noteworthy
HRJN96	Something noteworthy
JRWEYZ	Something noteworthy
KQZJPW	Something Noteworthy
L2Z97X	Something noteworthy
L78WJY	Something noteworthy
LDRZQ3	Something noteworthy
LUED6U	Something noteworthy
MK4BJT	Something noteworthy
P94MFP	Something noteworthy
PBRYEU	Something noteworthy
PRFA2W	Something noteworthy
PVHA3U	Something noteworthy
PZYA29	Something noteworthy
Q9J39W	Something noteworthy
QBL2JP	Something noteworthy

TABLE 1

Question 40	
WebCode	**Response**
QTQBNV	Something noteworthy
QZTKUN	Something noteworthy
RA9UVM	Something noteworthy
RWD889	Something noteworthy
T6DJYU	Something noteworthy
TGQJVM	Something Noteworthy
TL2WDL	Something noteworthy
U2P8ZN	Something noteworthy
UCYFWG	Something noteworthy
UM9CJR	Something noteworthy
UPZBXQ	Something noteworthy
UQBAVK	Something noteworthy
UTYLUQ	“Something noteworthy”
V6M9DQ	Something noteworthy
VJC6V2	Something Noteworthy
VU246Q	Something noteworthy
WJ3TAP	Something noteworthy
WX466N	Something noteworthy
X78WMG	Something noteworthy
X8ZRAP	something noteworthy
XJGCUL	Something noteworthy
XY9AWG	Something noteworthy
XYELUY	Something noteworthy
YQ9AWF	"Something Noteworthy"
Z8D34E	Something noteworthy
ZB38DY	Something noteworthy
ZX8VNE	Something noteworthy

TABLE 1

Question 40

Question 40: Provide the content of a note created with the notes app.

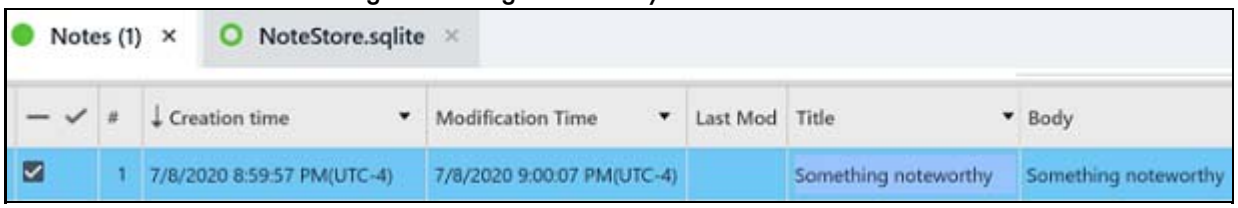
Consensus Result: Something noteworthy

Expected Response Explanation:

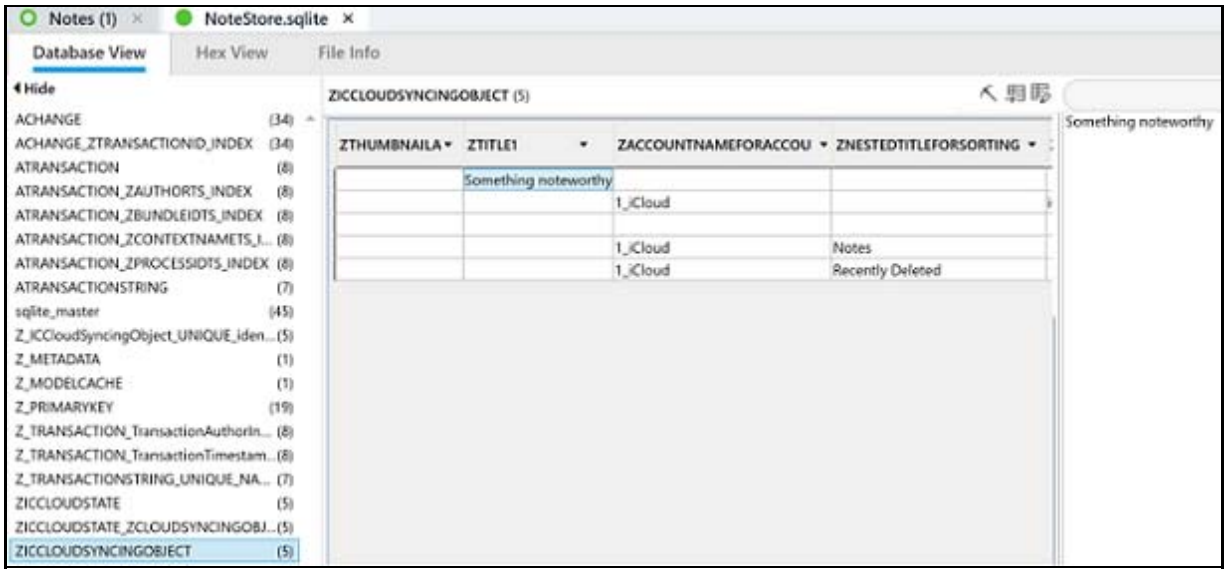
Notes are stored in /mobile/Containers/Shared/AppGroup/group.com.apple.notes/NoteStore.sqlite
Review of this file shows only one note, containing text, "Something noteworthy".

Expected Response Illustration:

Cellebrite "Note" view showing something noteworthy



Database view of NoteStore.sqlite showing something noteworthy



Additional Comments

TABLE 2

WebCode	Additional Comments
2MP2LK	Question 5 - In order to answer when a device was factory reset, you need a ".obliterated" file, which this image does not contain. When that happens, you can refer to the following databases as a "rule of thumb" for when a device was reset. SMS.db, voicemail.db, notes.sqlite, UserSettings.plist. Note that this does not guarantee that the device was reset though. It is notable that UserSettings.plist and notes.sqlite display different dates, although these files also are suggestive of a reset. Question 18 - If you use Celebrite Physical Analyzer, it reports the version number of 40.9.3. If you look at the mainfest.plist, it actually lists it as 4093. When you use additional tools, you can review the ch.protonmail.protonmail.plist which lists the version_preferred as 1.11.17 (4093). After reviewing the current ProtonMail iOS app on the AppStore, the current version is 1.12.3. Based on this information, the correct answer is 1.11.17. Question 24 - The answer is not formatted as in the question: The format in the answer (202) 762-1401, not 202-762-1401 as listed in the question.
3LXYYV	IMSI: 310260067723704, Last joined wifi Auto joined MAC Address 0:30:44:4:2F:4:B
7TZH7H	Question 8: Is the question about what the user sees on the phone (New York, U.S.A.) or how the same information is displayed in the phone's files (America/New_York) ? Question 18: The current version of Protonmail in the appstore is 1.12.3. The ProtonMail version on the phone is 1.1.17 and build version is 4093. Question 22: Only received SMS messages have "unread" status. Sent SMS messages are not counted.
8FY44R	The question about the "pager" number has two answers. James Roberts pager (202) 762-1401, source: AddressBook.sqlitedb. Mark pager: 12027621401, source: textnow. all date time answers were requested in the following format: using the following format: MM/DD/YYYY HH:MM AM/PM. however, however the device reported dates with HH:MM:SS. I reported all dates in device format. Google maps version was listed as: 5.46.7 all cellphone tools I know of require a physical dump to recover google maps data. I carved, and found an address?? maybe it's right. Did the flash fire when taking the photo captured on 6/28/2020 at 12:57:1. This question is difficult to answer... and a question of no real value. exif data shows: flash did not fire, auto mode but it was a yes, no answer only.
AJGDN9	For question 5 I used the date 07 05, 2020 which was located using the com.apple.purplebuddy.plist which contains the SetupLastExit date provided. This could be when the phone was turned on after the reset and there are other possible dates for the actual reset, such as 06 09, 2020 located from the creation time of the phones system files of the addressbook, sms.db and voicemail.db or the date of 07 08, 2020 located by the created date of the UserSettings.plist. As this is unclear on the specific date and time but one was required for the test I have noted these other possibilities here for completeness.
AUEEZC	For information search we used software "Cellebrite Physical Analyzer", version 7.35.2.16.
FNQKQ8	Forensic tool utilized: UFED Physical Analyzer 7.34.0.38
HRJN96	Several of the questions seemed to leave some type of interpretation. I would like to see more definitive questions. It seems that the person creating the test actually entered data but did not verify how the data was being displayed. This test is by far better than the previous test but I do see areas of improvement. I guess we will see how well I interpreted the questions when the results come back. I would like to also have the ability to upload the results from my answers which include screen captures of where I found the data and how I came to my conclusion. Which may help in developing/verifying the results.

TABLE 2

WebCode	Additional Comments
KQZJPW	In a few of the answers, I entered a bit of additional information to accurately present my answer.
L78WJY	Some questions give very exact formatting for how the answer should be given like in number 1 but others could be better explained like number 31 which just asks to describe what is being shown. It is a funny joke but do you want me to describe the whole video and its contents or is my answer of just a music video sufficient?
QTQBNV	For Question #5, cannot tell for certain because .obliterated file is not present since this was not a physical extraction. For Question #35. The web visit in safari to a https://news.google.com/topstories?hl=en-US&gl=US&ceid=US:en was last visited on 7/5/2020 13:07(UTC-4). My answer to question #35 is in reference to your exact web address that was listed in the question (http://news.google.com/).
TGQJVM	Question 32, the question was worded awkwardly. I believe it to mean a searched for address using the google maps app. Either way, no address could be found in regards to google maps. Question 39, timestamp was a bit off. I chose the 9:52:56 as it was closest to the time asked.
TL2WDL	BTW, I appreciate being Rick-Rolled. I actually guffawed.
U2P8ZN	For Question 5 on the files used to identify when the device was reset, the files used to identify this date had either June 9, 2020 if UTC-4 or June 10, 2020 if UTC+0. The question didn't clarify what time zone to choose. For Question 10, the forensic tool used to process the extraction reported the MSISDN in two different formats so I have included both, 17036658672 and +1 (703) 665-8672. For Question 23, where did he device owner agree to meet, I left the '?' at the end of Lafayette square because the instructions for the test say that answers must be reported exactly as found within the evidence and to provide the complete body for text, not to condense the answer. For Question 31, I wasn't sure if the context of the file meant it was a multimedia file/video file or a description of what the video was about, so I put a video file of Rick Astley singing Never Gonna Give You Up. For Question 36, I was unsure if what type of payment card website meant the actual name of the card/website, being 'MyVanillaCard' or that its a Reloadable Prepaid Card so my answer included the entirety of the card description MyVanilla Reloadable Prepaid Card
Z8D34E	3: What method/type of extraction was performed? (which answer to provide is not clear) Cellebrite, ExtractionType=Logical, ExtractionMethod=iPhone 6s, UFEDExtractionMethod=Ufed, AppleDevice_AdvancedLogical. 6: What is the model name of this phone (e.g. iPhone 4c)? (could provide multiple answers, based on the example stayed with that scheme) N71AP / iPhone 6s / iPhone8,1. 8: What is the set time zone for this phone? Provide answer exactly as shown by the device.(this can be sources from more then one location) obvious answer would be from the plist file PA gets the data from and displays in extraction summary, but also the local time file. 14: What is the SSID (name) of the LAST WiFi Hotspot connected to this phone? (the word "hotspot" may confuse some as it is on the name of artifacts, can't tell if that was purpose of the question) MBR-f4b. 29: With what service or application is the number 2029459404 associated? (this questions has two answers, it could also be TextNow) ProtonMail

-End of Report-
(Appendix may follow)