



Mobile Digital Evidence - iOS Analysis Test No. 18-5551 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 was returned from 52 participants and are compiled in the following tables:

	<u>Page</u>
1: Manufacturer's Information	2
2: Summary Comments	6
3: Table 1: Digital Evidence Responses	7
4: Table 2: Additional Comments	79

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 an iPhone in .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 on an assisted suicide incident was created to generate user data on the evidence device. The execution of the scripted scenario took place the week of May 21, 2018. An Apple iPhone 6 phone was used to perform the activities and generate the intended artifacts.

The phone data was acquired through an advanced logical extraction of the iPhone 6 utilizing Cellebrite software. Following sample validation, a .tar file was uploaded to the CTS portal for participants to download. MD5 and SHA-1 algorithms were run on the compressed folder to generate unique hash values to allow participants to validate the successful download of the files.

SAMPLE VALIDATION/VERIFICATION:

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

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

SCENARIO PROVIDED TO PARTICIPANTS

Police are investigating a possible homicide/suicide case. A Matthew Thyne was found hanging dead in his room by his parents. Police responded to the crime scene and collected all the evidence. Along with other evidence, police collected Matthew Thyne's iPhone and logged it into evidence. A logical image of the iPhone was created and you have been tasked with analyzing the forensic image of the iPhone utilizing your own tools and methods to find any evidence that could be of interest to the police.

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Expected Response</u>
1	<u>Provide the MD5 hash value for the iPhoneBackup.tar file.</u> <i>b8ffc5ccfb8ebbd438d07bd0d30d592</i>
2	<u>Provide the SHA1 (base 16) hash value for the iPhoneBackup.tar file.</u> <i>bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d</i>
3	<u>What is the set time zone for this device? Provide the answer in the following format: Country/State</u> <i>America/New_York</i>
4	<u>What is the 19 digit ICCID number associated with the device?</u> <i>8901260155718778937</i>
5	<u>What is the model number of the device?</u> <i>MG5W2</i>
6	<u>What is the version of the operating system on this device?</u> <i>11.2</i>
7	<u>Based on the calendar events, when is the event "School Trip" scheduled for? Provide the answer in the following format: MM/DD/YYYY</u> <i>07/04/2018 and/or 07/05/2018</i>
8	<u>How many contacts were saved on the device? Do not include contacts from third party applications or duplicated contacts.</u> <i>Three (3)</i>
9	<u>Provide the phone number associated with contact named "Mom".</u> <i>(703) 568-1862</i>
10	<u>Were location services enabled on this device?</u> <i>Yes</i>
11	<u>Who was the service provider for this number?</u> <i>T-Mobile</i>
12	<u>Provide the name (SSID) of the location this device was last connected to using Wi-Fi.</u> <i>Walmartwifi</i>
13	<u>Provide the phone number associated with this device.</u> <i>(202) 378-7266</i>
14	<u>Based on the evidence, which two medications were prescribed to the user? Separate the medications with a comma (,)</u> <i>Celexa, Lexapro</i>

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Expected Response</u>
15 <u>What is the version of ExpediaBookings application installed on this device?</u>	33.8.1
16 <u>What is the version of the Skype application installed on this device?</u>	8.21.0.7
17 <u>What is the user's Skype username? Provide the answer using the following format: live:_____</u>	live:Thyne13
18 <u>What is the user's Facebook login email ID?</u>	mthyne13@gmail.com
19 <u>What is the user's Facebook password?</u>	Polarbear13
20 <u>Based on the evidence, what is the home address for Annie Fao? Provide the Street, City, State, and Zip code. (Ex: 1234 Adams St., Chester, FL 10056)</u>	16444 Atlanta Drive, Fairfax, VA 20091
21** <u>Provide the longitude and latitude of the last place viewed using Google Maps Application. Answer using the following format: Longitude: _____, Latitude: _____</u>	Longitude: -77.3967717728168, Latitude: 38.8548381516278
22 <u>What was the last phrase searched using the Safari search engine?</u>	ways to commit suicide
23 <u>Provide the email ID which is associated with the user's iCloud account.</u>	thyne13@icloud.com
24 <u>What is the password of the iCloud account on this device?</u>	2019Graduate
25 <u>How many voicemails were received from +1 571-484-0504?</u>	Two (2)
26 <u>Other than iMessages, which 3rd party chat application did the user primarily use to send and receive messages from +1 571-484-0504?</u>	WhatsApp
27 <u>To whom was the last phone call placed using this device? Provide the first and last name. (First Last)</u>	Annie Fao

Manufacturer's Information, continued

- | <u>Question</u> | <u>Manufacturer's Expected Response</u> |
|-----------------|--|
| 28 | <u>What was the type of the last outgoing call placed using this device? Choose one of the following: Voice call, FaceTime</u>
<i>FaceTime</i> |
| 29 | <u>What is the duration of the last outgoing (audio or video) call? Answer using the following format: hh:mm:ss</u>
<i>00:08:06</i> |
| 30 | <u>Provide the contents of the last message SENT TO Annie Fao via WhatsApp Application on 5/24/2018.</u>
<i>Yes I know. I will call you in a few minutes.</i> |
| 31 | <u>Provide the contents of the last message RECEIVED FROM Annie Fao via WhatsApp Application on 5/24/2018.</u>
<i>Your parents should be back soon. We need to do this fast!</i> |
| 32** | <u>The user shared their location on 5/24/2018 10:53 AM(UTC-4) using WhatsApp Application. Provide the latitude and longitude of the shared location. Answer using the following format: Longitude: _____, Latitude: _____</u>
<i>Longitude: -77.396728515625, Latitude: 38.8545341491699</i> |
| 33** | <u>Provide the creation time of the multimedia file named "IMG_0023.MOV". Answer using the time zone set on the device in the following format: Month / Day / Year, Hours: Minutes: Seconds AM / PM.</u>
<i>5/21/2018 03:24:54 PM</i> |
| 34 | <u>What type of file was received from + 1 571-484-0504 on May 23, 2018 at 3:33:23 PM GMT-04:00 via WhatsApp application. Provide the file extension of the file. (Ex: .docx)</u>
<i>.JPG</i> |
| 35 | <u>What is the make and model of the camera used to capture IMG_0035.JPG? Provide the answer in the following format: Make: _____, Model: _____</u>
<i>Make: Apple, Model: iPhone6</i> |
| 36 | <u>Which web search browser was used to download "IMG_0024.PNG"? Choose one of the following: Chrome, Safari</u>
<i>Safari</i> |

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: image details, phone and network settings, applications, communications, web browser history, and Geo-Location information.

Out of thirty six (36) questions, three (3) questions did not reach a clear consensus. Two of the three questions dealt with GPS coordinates. For these questions (#21 and #32), participants were asked to provide the Latitude and Longitude coordinates of a particular location. We found that the participants reported the expected coordinates, however, they labeled the latitude coordinates as longitude and longitude as latitude.

The third question (#33) was a date/time question where participants were asked to provide the creation time of a file in the time zone set on the device. This question did not reach consensus because the results were provided in different time zones.

Detailed explanation, file path, and screenshots of results can be found within Table 1, under the "Expected Response Explanation" section for each question.

Digital Evidence Responses

TABLE 1

Question 1 - Authentication

Question 1: Provide the MD5 hash value for the iPhoneBackup.tar file.

Manufacturer's Expected Response: b8ffc5ccfb8ebbd438d07fbd0d30d592

WebCode	Response
22YJRM	b8ffc5ccfb8ebbd438d07fbd0d30d592
2PK3JP	B8FFC5CCFB8EBBD438D07FBD0D30D592
2UUKEC	b8ffc5ccfb8ebbd438d07fbd0d30d592
42996J	b8ffc5ccfb8ebbd438d07fbd0d30d592
4CQRKA	b8ffc5ccfb8ebbd438d07fbd0d30d592
4N7HNL	65b5902462131bbbb97d1fa34a1bf0ea
6VXEL8	B8FFC5CCFB8EBBD438D07FBD0D30D592
7W9GAR	b8ffc5ccfb8ebbd438d07fbd0d30d592
7WNX6K	b8ffc5ccfb8ebbd438d07fbd0d30d592
7YP3H6	b8ffc5ccfb8ebbd438d07fbd0d30d592
88MVQY	b8ffc5ccfb8ebbd438d07fbd0d30d592
94JJ86	B8FFC5CCFB8EBBD438D07FBD0D30D592
94W9BG	b8ffc5ccfb8ebbd438d07fbd0d30d592
9UUTMX	B8FFC5CCFB8EBBD438D07FBD0D30D592
A2Q6XK	B8FFC5CCFB8EBBD438D07FBD0D30D592
ATHB7D	b8ffc5ccfb8ebbd438d07fbd0d30d592
B3XPLK	b8ffc5ccfb8ebbd438d07fbd0d30d592
B4U49D	B8FFC5CCFB8EBBD438D07FBD0D30D592
CEB8TH	b8ffc5ccfb8ebbd438d07fbd0d30d592
CW7WPB	B8FFC5CCFB8EBBD438D07FBD0D30D592
D2H6QF	b8ffc5ccfb8ebbd438d07fbd0d30d592
DBKM2J	B8FFC5CCFB8EBBD438D07FBD0D30D592
DPMTFN	B8FFC5CCFB8EBBD438D07FBD0D30D592
DR6DZH	b8ffc5ccfb8ebbd438d07fbd0d30d592
EZ2BMK	b8ffc5ccfb8ebbd438d07fbd0d30d592
FA2K8F	b8ffc5ccfb8ebbd438d07fbd0d30d592
FML3XX	B8FFC5CCFB8EBBD438D07FBD0D30D592
FV2JUE	b8ffc5ccfb8ebbd438d07fbd0d30d592
FWCHNM	B8FFC5CCFB8EBBD438D07FBD0D30D592
LVHNTE	b8ffc5ccfb8ebbd438d07fbd0d30d592
NQGLFN	65b5902462131bbbb97d1fa34a1bf0ea
PBMBAX	B8FFC5CCFB8EBBD438D07FBD0D30D592
PFELHB	B8FFC5CCFB8EBBD438D07FBD0D30D592
Q37ZWW	b8ffc5ccfb8ebbd438d07fbd0d592
REWD8D	b8ffc5ccfb8ebbd438d07fbd0d30d592

TABLE 1

Question 1 - Authentication	
WebCode	Response
RWF8X3	b8ffc5ccfb8ebbd438d07fbd0d30d592
TF6KA7	b8ffc5ccfb8ebbd438d07fbd0d30d592
UMXFKA	b8ffc5ccfb8ebbd438d07fbd0d30d592
UZMCL8	B8FFC5CCFB8EBBD438D07FBD0D30D592
V3PCKJ	B8FFC5CCFB8EBBD438D07FBD0D30D592
V8MVLH	b8ffc5ccfb8ebbd438d07fbd0d30d592
VFWK22	b8ffc5ccfb8ebbd438d07fbd0d30d592
VNNZQ6	65b5902462131bbbb97d1fa34a1bf0ea
WKJPAV	65b5902462131bbbb97d1fa34a1bf0ea
WMDDTR	B8FFC5CCFB8EBBD438D07FBD0D30D592
WUUUHF	b8ffc5ccfb8ebbd438d07fbd0d30d59
XMPFC6	b8ffc5ccfb8ebbd438d07fbd0d30d592
XMTWCN	b8ffc5ccfb8ebbd438d07fbd0d30d592
XX9QNG	B8FFC5CCFB8EBBD438D07FBD0D30D592
Y4U2D7	65b5902462131bbbb97d1fa34a1bf0ea
ZE9HK3	b8ffc5ccfb8ebbd438d07fbd0d30d592
ZNEHVP	B8FFC5CCFB8EBBD438D07FBD0D30D592

Consensus Result: b8ffc5ccfb8ebbd438d07fbd0d30d592

Expected Response Explanation:

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

Expected Response Illustration:

MD5 Hash Value:

<input checked="" type="checkbox"/> MD5	b8ffc5ccfb8ebbd438d07fbd0d30d592
---	----------------------------------

TABLE 1

Question 2 - Authentication

Question 2: Provide the SHA1 (base 16) hash value for the iPhoneBackup.tar file.

Manufacturer's Expected Response: bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d

WebCode	Response
22YJRM	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
2PK3JP	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
2UUKEC	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
42996J	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
4CQRKA	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
4N7HNL	75410ca9ecc54aee7da54ac6ead90f1158f06e64
6VXEL8	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
7W9GAR	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
7WNX6K	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
7YP3H6	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
88MVQY	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
94JJ86	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
94W9BG	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
9UUTMX	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
A2Q6XK	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
ATHB7D	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
B3XPLK	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
B4U49D	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
CEB8TH	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
CW7WPB	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
D2H6QF	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
DBKM2J	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
DPMTFN	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
DR6DZH	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
EZ2BMK	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
FA2K8F	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
FML3XX	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
FV2JUE	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
FWCHNM	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
LVHNTE	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
NQGLFN	75410ca9ecc54aee7da54ac6ead90f1158f06e64
PBMBAX	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
PFELHB	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
Q37ZWW	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
REWD8D	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
RWF8X3	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
TF6KA7	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d

TABLE 1

Question 2 - Authentication	
WebCode	Response
UMXFKA	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
UZMCL8	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
V3PCKJ	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
V8MVLH	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
VFWK22	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
VNNZQ6	75410ca9ecc54aee7da54ac6ead90f1158f06e64
WKJPAV	75410ca9ecc54aee7da54ac6ead90f1158f06e64
WMDDTR	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
WUUUHF	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
XMPFC6	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
XMTWCN	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
XX9QNG	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D
Y4U2D7	75410ca9ecc54aee7da54ac6ead90f1158f06e64
ZE9HK3	bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d
ZNEHVP	BC4877C5948652F4AF3CC2BB5A82F79D0C6F8D1D

Consensus Result: bc4877c5948652f4af3cc2bb5a82f79d0c6f8d1d

Expected Response Explanation:

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

Expected Response Illustration:

SHA1 Hash Value:

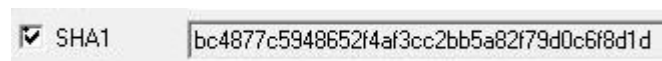


TABLE 1

Question 3 - Features/Settings

**Question 3: What is the set time zone for this device? Provide the answer in the following format:
Country/State**

Manufacturer's Expected Response: America/New_York

WebCode	Response
22YJRM	America/New York
2PK3JP	America/New_York
2UUKEC	America/New York
42996J	(UTC-05:00) New_York (America)
4CQRKA	America/New_York
4N7HNL	America, New York
6VXEL8	America/New_York
7W9GAR	America (USA)/New York
7WNX6K	America/New_York
7YP3H6	America/New_York
88MVQY	America/New York
94JJ86	America/New_York
94W9BG	America/New York
9UUTMX	America/New York
A2Q6XK	America/New_York
ATHB7D	America/New York
B3XPLK	America/New York
B4U49D	America/New_York
CEB8TH	America/New_York
CW7WPB	America/New York
D2H6QF	America/New York
DBKM2J	(UTC-05:00) New_York (America)
DPMTFN	America/New_York
DR6DZH	America/New_York
EZ2BMK	America/New_York
FA2K8F	America/New York
FML3XX	America/New_York
FV2JUE	America/New York
FWCHNM	America/New_York
LVHNTTE	America/New York
NQGLFN	America/New York
PBMBAX	America/New York
PFELHB	America/New_York
Q37ZWW	America/New York
REWD8D	America/New_York
RWF8X3	New York/America
TF6KA7	America/New_York

TABLE 1

Question 3 - Features/Settings	
WebCode	Response
UMXFKA	America/New_York
UZMCL8	America/New_York
V3PCKJ	America/New_York
V8MVLH	America/New_York
VFWK22	America/New_York
VNNZQ6	America/New York
WKJPAV	America/New York
WMDDTR	America/New York
WUUUHF	America/New_York
XMPFC6	America/New York
XMTWCN	America/New York
XX9QNG	America/New_York
Y4U2D7	America/ New York
ZE9HK3	America/New York
ZNEHVP	AMERICA/NEW_YORK

Consensus Result: America/New_York

Expected Response Explanation:

The time zone set on this device can be found in the device_values.plist. It can also be verified by looking at the time stamps of various data including Email, Call Log, and Text Messages.

Expected Response Illustration:

TimeZone at offset 0x13FF

```

3E 54 69 6D 65 5A 6F 6E 65 | >TimeZone
3C 2F 6B 65 79 3E 0A 09 3C | </key>..<
73 74 72 69 6E 67 3E 41 6D | string>Am
65 72 69 63 61 2F 4E 65 77 | erica/New
5F 59 6F 72 6B 3C 2F 73 74 | York</st
    
```

TABLE 1

Question 4 - Features/Settings

Question 4: What is the 19 digit ICCID number associated with the device?

Manufacturer's Expected Response: 8901260155718778937

WebCode	Response
22YJRM	8901260155718778937
2PK3JP	8901260155718778937
2UUKKC	8901260155718778937
42996J	8901260155718778937
4CQRKA	8901260155718778937
4N7HNL	8901260155718778937
6VXEL8	8901260155718778937
7W9GAR	8901260155718778937
7WNX6K	8901260155718778937
7YP3H6	8901260155718778937
88MVQY	8901260155718778937
94JJ86	8901260155718778937
94W9BG	8901260155718778937
9UUTMX	8901260155718778937
A2Q6XK	8901260155718778937
ATHB7D	8901260155718778937
B3XPLK	8901260155718778937
B4U49D	8901260155718778937
CEB8TH	8901260155718778937
CW7WPB	8901260155718778937
D2H6QF	8901260155718778937
DBKM2J	8901260155718778937
DPMTFN	8901260155718778937
DR6DZH	8901260155718778937
EZ2BMK	8901260155718778937
FA2K8F	8901260155718778937
FML3XX	8901260155718778937
FV2JUE	8901260155718778937
FWCHNM	8901260155718778937
LVHNTTE	8901260155718778937
NQGLFN	8901260155718778937
PBMBAX	8901260155718778937
PFELHB	8901260155718778937
Q37ZWW	8901260155718778937
REWD8D	8901260155718778937
RWF8X3	8901260155718778937
TF6KA7	8901260155718778937

TABLE 1

Question 4 - Features/Settings	
WebCode	Response
UMXFKA	8901260155718778937
UZMCL8	8901260155718778937
V3PCKJ	8901260155718778937
V8MVLH	8901260155718778937
VFWK22	8901260155718778937
VNNZQ6	8901260155718778937
WKJPAV	8901260155718778937
WMDDTR	8901260155718778937
WUUUHF	8901260155718778937
XMPFC6	8901260155718778937
XMTWCN	8901260155718778937
XX9QNG	8901260155718778937
Y4U2D7	8901260155718778937
ZE9HK3	8901260155718778937
ZNEHVP	8901260155718778937

Consensus Result: 8901260155718778937

Expected Response Explanation:

The unique Integrated Circuit Card Identifier (ICCID) can found within the Info.plist file at offset 0x174.

Expected Response Illustration:

19 Digital ICCID Number:

```

3E 49 43 43 49 44 3C | >ICCID<
2F 6B 65 79 3E 0A 09 | /key>..
3C 73 74 72 69 6E 67 | <string
3E 38 39 30 31 32 36 | >890126
30 31 35 35 37 31 38 | 0155718
37 37 38 39 33 37 3C | 778937<
    
```

TABLE 1

Question 5 - Features/Settings

Question 5: What is the model number of the device?

Manufacturer's Expected Response: MG5W2

WebCode	Response
22YJRM	iPhone 6
2PK3JP	MG5W2
2UUKEC	MG5W2
42996J	MG5W2
4CQRKA	MG5W2
4N7HNL	MG5W2
6VXEL8	MG5W2
7W9GAR	MG5W2 (iPhone 6)
7WNX6K	MG5W2
7YP3H6	MG5W2
88MVQY	MG5W2
94JJ86	MG5W2
94W9BG	MG5W2
9UUTMX	iPhone 6
A2Q6XK	MG5W2
ATHB7D	MG5W2
B3XPLK	iPhone 6, Model number N61AP
B4U49D	iPhone 6
CEB8TH	MG5W2
CW7WPB	MG5W2
D2H6QF	Model number: MG5W2
DBKM2J	MG5W2
DPMTFN	MG5W2
DR6DZH	MG5W2
EZ2BMK	MG5W2
FA2K8F	iPhone 6 MG5W2
FML3XX	A1549 iPhone 6 (MG5W2 iPhone7,2)
FV2JUE	MG5W2
FWCHNM	MG5W2
LVHNTTE	MG5W2
NQGLFN	MG5W2
PBMBAX	MG5W2
PFELHB	MG5W2
Q37ZWW	iPhone 7,2
REWD8D	iPhone 6 (A1549)
RWF8X3	MG5W2
TF6KA7	MG5W2

TABLE 1

Question 5 - Features/Settings	
WebCode	Response
UMXFKA	MG5W2
UZMCL8	MG5W2
V3PCKJ	iPhone 6
V8MVLH	MG5W2
VFWK22	MG5W2
VNNZQ6	iPhone7,2
WKJPAV	MG5W2
WMDDTR	MG5W2
WUUUHF	MG5W2
XMPFC6	MG5W2
XMTWCN	The model number was found to be: "MG5W2" and the detected phone model: "iPhone 6 (A1549, A1586)"
XX9QNG	MG5W2
Y4U2D7	MG5W2
ZE9HK3	A1549
ZNEHVP	MG5W2 iPhone6 iPhone7,2

Consensus Result: MG5W2

Expected Response Explanation:

The model number of this device can be found in the device_values.plist at offset 0xFA9.

Expected Response Illustration:

Model Number:

```

4D 6F 64 65 6C | key>Model
65 72 3C 2F 6B | Number</k
09 3C 73 74 72 | ey>..<str
4D 47 35 57 32 | ing>MG5W2
    
```


TABLE 1

Question 6 - Features/Settings

Question 6: What is the version of the operating system on this device?

Manufacturer's Expected Response: 11.2

WebCode	Response
22YJRM	11.2
2PK3JP	11.2
2UUKEC	11.2
42996J	iOS 11.2
4CQRKA	11.2
4N7HNL	11.2
6VXEL8	11.2
7W9GAR	IOS 11.2
7WNX6K	11.2
7YP3H6	11.2
88MVQY	11.2
94JJ86	11.2
94W9BG	11.2
9UUTMX	11.2
A2Q6XK	11.2
ATHB7D	11.2
B3XPLK	iOS 11.2
B4U49D	11.2
CEB8TH	11.2
CW7WPB	11.2
D2H6QF	iOS 11.2
DBKM2J	11.2
DPMTFN	11.2
DR6DZH	11.2
EZ2BMK	11.2
FA2K8F	11.2
FML3XX	11.2
FV2JUE	11.2
FWCHNM	11.2
LVHNTTE	11.2
NQGLFN	11.2
PBMBAX	11.2
PFELHB	11.2
Q37ZWW	11.2
REWD8D	11.2
RWF8X3	11.2
TF6KA7	11.2

TABLE 1

Question 6 - Features/Settings	
WebCode	Response
UMXFKA	11.2
UZMCL8	11.2
V3PCKJ	11.2
V8MVLH	11.2
VFWK22	11.2
VNNZQ6	6.30.04
WKJPAV	OS 11.2
WMDDTR	11.2
WUUUHF	11.2
XMPFC6	11.2
XMTWCN	iOS version: "OS Version 11.2" and "Revision 11.2 (15C114)"
XX9QNG	11.2
Y4U2D7	11.2
ZE9HK3	11.2
ZNEHVP	11.2

Consensus Result: 11.2

Expected Response Explanation:

The operating system version can be found in the device_values.plist at offset 0x10B5.

Expected Response Illustration:

OS Version:

ProductVersion : string = 11.2

TABLE 1

Question 7 - Features/Settings

Question 7: Based on the calendar events, when is the event "School Trip" scheduled for? Provide the answer in the following format: MM/DD/YYYY

Manufacturer's Expected Response: 07/04/2018 and/or 07/05/2018

WebCode	Response
22YJRM	07/04/2018
2PK3JP	07/04/2018
2UUKEC	07/04/2018
42996J	07/05/2018
4CQRKA	07/04/2018
4N7HNL	07/04/2018
6VXEL8	07/05/2018
7W9GAR	07/04/2018 19:00(UTC-5) 07/05/2018 18:59(UTC-5)
7WNX6K	07/05/2018
7YP3H6	07/04/2018 8:00:00 PM (UTC-4)
88MVQY	07/04/2018
94JJ86	07/04/2018
94W9BG	07/04/2018
9UUTMX	7/4/2018 8:00:00 PM(UTC-4) (Start Date) 7/5/2018 7:59:59 PM(UTC-4) (End Date)
A2Q6XK	07/04/2018
ATHB7D	07/05/2018
B3XPLK	07/05/2018
B4U49D	07/04/2018
CEB8TH	07/04/2018 20:00:00 (UTC-4)
CW7WPB	07/04/2018
D2H6QF	07/04/2018 20:00:00 GMT-04:00 - 07/05/2018 19:59:59 GMT-04:00
DBKM2J	07/04/2018-07/05/2018
DPMTFN	07/05/2018
DR6DZH	04/07/2018
EZ2BMK	07/04/2018
FA2K8F	07/05/2018
FML3XX	07/05/2018
FV2JUE	07/05/2018
FWCHNM	07/05/2018
LVHNTTE	07/04/2018
NQGLFN	07/04/2018 – 07/05/2018
PBMBAX	07/05/2018
PFELHB	07/04/2018
Q37ZWW	07/04/2018
REWD8D	07/04/2018
RWF8X3	07/04/2018
TF6KA7	07/04/2018

TABLE 1

Question 7 - Features/Settings	
WebCode	Response
UMXFKA	07/04/2018
UZMCL8	7/5/2018
V3PCKJ	07/04/2018
V8MVLH	07/05/2018
VFWK22	07/04/2018
VNNZQ6	07/05/2018
WKJPAV	07/05/2018
WMDDTR	07/04/2018
WUUUHF	07/05/2018
XMPFC6	07/05/2018
XMTWCN	It would appear that the event "School Trip" is scheduled for 07/05/2018.
XX9QNG	07/04/2018
Y4U2D7	07/04/2018
ZE9HK3	07/04/2018
ZNEHVP	07/04/2018

Consensus Result: 07/04/2018 and/or 07/05/2018

Expected Response Explanation:

The calendar event "School Trip" can be found within the Calendar.sqlitedb (offset 0x80285) which is located at: /var/mobile/Library/Calendar/Calendar.sqlitedb.

This event had a different start date and end date. Since the question did not specify start or end date, both answers were accepted for this question.

Expected Response Illustration:

Start Date:

Hex dump showing memory addresses and values for the start date field. The values 20 ED 97 00 correspond to the date 7/4/2018. A screenshot of the calendar entry shows the start date as 7/4/2018 08:00 PM(UTC-4).

End Date:

Hex dump showing memory addresses and values for the end date field. The values 20 EE E8 7F correspond to the date 7/5/2018. A screenshot of the calendar entry shows the end date as 7/5/2018 07:59 PM(UTC-4).

TABLE 1

Question 8 - Features/Settings	
--------------------------------	--

Question 8: How many contacts were saved on the device? Do not include contacts from third party applications or duplicated contacts.

Manufacturer's Expected Response: Three (3)

WebCode	Response
22YJRM	3
2PK3JP	3
2UUKEC	3
42996J	3
4CQRKA	3
4N7HNL	Three (3)
6VXEL8	3
7W9GAR	3
7WNX6K	3
7YP3H6	3
88MVQY	3
94JJ86	3
94W9BG	3
9UUTMX	3
A2Q6XK	3
ATHB7D	3
B3XPLK	3
B4U49D	3
CEB8TH	3
CW7WPB	3
D2H6QF	3
DBKM2J	3
DPMTFN	3
DR6DZH	3
EZ2BMK	3
FA2K8F	3
FML3XX	3
FV2JUE	3
FWCHNM	3
LVHNTTE	3
NQGLFN	3
PBMBAX	3
PFELHB	3
Q37ZWW	3
REWD8D	3
RWF8X3	3
TF6KA7	3

TABLE 1

Question 8 - Features/Settings	
WebCode	Response
UMXFKA	3
UZMCL8	3
V3PCKJ	3
V8MVLH	3
VFWK22	3
VNNZQ6	3
WKJPAV	Three (3)
WMDDTR	3
WUUUHF	3
XMPFC6	3
XMTWCN	3
XX9QNG	3
Y4U2D7	3
ZE9HK3	3
ZNEHVP	3

Consensus Result: Three (3)

Expected Response Explanation:

There were a total of three contacts saved on the device. The saved contacts can be found within the AddressBook.sqlitedb which can be located at: /var/mobile/Library/AddressBook/AddressBook.sqlitedb

Expected Response Illustration:

Contacts:

↑ Name ▼	Phones
Annie Fao	Home (571) 484-0504
Dad	Home (571) 415-7357
Mom	Home (703) 568-1862

TABLE 1

Question 9 - Features/Settings	
--------------------------------	--

Question 9: Provide the phone number associated with contact named "Mom".

Manufacturer's Expected Response: (703) 568-1862

WebCode	Response
22YJRM	(703) 568-1862
2PK3JP	(703) 568-1862
2UUKEC	(703) 568-1862
42996J	(703) 568-1862
4CQRKA	(703) 568-1862
4N7HNL	(703) 568-1862
6VXEL8	(703) 568-1862
7W9GAR	(703) 568-1862
7WNX6K	(703) 568-1862
7YP3H6	703-568-1862
88MVQY	(703) 568-1862
94JJ86	(703) 568-1862
94W9BG	(703)568-1862
9UUTMX	(703) 568-1862
A2Q6XK	(703) 568-1862
ATHB7D	(703)568-1862
B3XPLK	(703) 568-1862
B4U49D	7035681862
CEB8TH	(0703)568-1862
CW7WPB	(703)568-1862
D2H6QF	(703) 568-1862
DBKM2J	(703) 568-1862
DPMTFN	(703) 568-1862
DR6DZH	(703) 568-1862
EZ2BMK	(703) 568-1862
FA2K8F	(703) 568-1862
FML3XX	703-568-1862
FV2JUE	(703) 568-1862
FWCHNM	(703) 568-1862
LVHNTTE	703-568-1862
NQGLFN	+1 703-568-1862
PBMBAX	(703) 568-1862
PFELHB	703-568-1862
Q37ZWW	(703) 568-1862
REWD8D	(703) 568-1862
RWF8X3	(703) 568-1862
TF6KA7	(703) 568-1862

TABLE 1

Question 9 - Features/Settings	
WebCode	Response
UMXFKA	(703) 568-1862
UZMCL8	(703)568-1862
V3PCKJ	(703) 568-1862
V8MVLH	703-568-1862
VFWK22	703-568-1862
VNNZQ6	703-568-1862
WKJPAV	(703) 568-1862
WMDDTR	(703) 568-1862
WUUUHF	703-568-1862
XMPFC6	(703)568-1862
XMTWCN	(703) 568-1862
XX9QNG	(703) 568-1862
Y4U2D7	(703) 568-1862
ZE9HK3	(703) 568-1862
ZNEHVP	(703)568-1862

Consensus Result: (703) 568-1862

Expected Response Explanation:

The phone number for contact named "Mom" can be found within the AddressBook.sqlitedb which can be located at: /var/mobile/Library/AddressBook/AddressBook.sqlitedb

Expected Response Illustration:

Contact number for "Mom"

↑ Name ▾	Phones ▾
Mom	Home (703) 568-1862

TABLE 1

Question 10 - Features/Settings	
---------------------------------	--

Question 10: Were location services enabled on this device?

Manufacturer's Expected Response: Yes

WebCode	Response
22YJRM	Yes
2PK3JP	Yes
2UUKEC	Yes
42996J	yes
4CQRKA	Yes
4N7HNL	YES
6VXEL8	Yes
7W9GAR	Yes
7WNX6K	yes
7YP3H6	Yes
88MVQY	Yes
94JJ86	Yes
94W9BG	Yes
9UUTMX	Yes
A2Q6XK	Yes
ATHB7D	Enabled
B3XPLK	Yes
B4U49D	yes
CEB8TH	Yes
CW7WPB	Yes
D2H6QF	Yes
DBKM2J	Yes.
DPMTFN	yes
DR6DZH	Yes
EZ2BMK	Yes
FA2K8F	Yes
FML3XX	Yes
FV2JUE	Yes
FWCHNM	Yes
LVHNTTE	Yes
NQGLFN	Yes
PBMBAX	Yes
PFELHB	YES
Q37ZWW	Yes
REWD8D	Yes
RWF8X3	Yes
TF6KA7	Yes

TABLE 1

Question 10 - Features/Settings	
WebCode	Response
UMXFKA	Yes
UZMCL8	Yes
V3PCKJ	Yes
V8MVLH	Yes
VFWK22	Yes
VNNZQ6	Yes
WKJPAV	Yes
WMDDTR	Yes
WUUUHF	Yes
XMPFC6	Yes
XMTWCN	Yes, True
XX9QNG	Yes
Y4U2D7	Yes
ZE9HK3	Yes
ZNEHVP	YES

Consensus Result: Yes

Expected Response Explanation:

The location settings for this device can be found within the apple.locationd.plist file which is located at:
/var/mobile/Library/Preferences/com.apple.locationd.plist

Expected Response Illustration:

Location Settings:

`LocationServicesEnabledIn8.0 : integer = 1`

TABLE 1

Question 11 - Features/Settings

Question 11: Who was the service provider for this number?

Manufacturer's Expected Response: T-Mobile

WebCode	Response
22YJRM	T-Mobile
2PK3JP	T-Mobile
2UUKEC	T-Mobile
42996J	T-Mobile
4CQRKA	T-Mobile
4N7HNL	T-Mobile
6VXEL8	T-Mobile
7W9GAR	T-MOBILE
7WNX6K	T-Mobile
7YP3H6	T-Mobile
88MVQY	T-Mobile
94JJ86	T-Mobile
94W9BG	T-Mobile
9UUTMX	It depends on which number is meant by "this number"; if it's Mom's phone number then WhatsApp is the service provider. If it's the phone number for the actual phone in question then T-Mobile is the answer.
A2Q6XK	T-Mobile USA
ATHB7D	T-Mobile
B3XPLK	T-Mobile USA
B4U49D	T-Mobile
CEB8TH	T-Mobile
CW7WPB	T-Mobile
D2H6QF	T-Mobile
DBKM2J	T-Mobile.
DPMTFN	T-Mobile
DR6DZH	T-Mobile
EZ2BMK	T-Mobile
FA2K8F	T-Mobile (US)
FML3XX	T-Mobile
FV2JUE	T-Mobile
FWCHNM	T-Mobile
LVHNTTE	T-Mobile
NQGLFN	T-Mobile
PBMBAX	T-Mobile
PFELHB	T-MOBILE
Q37ZWW	T-Mobile
REWD8D	T-Mobile
RWF8X3	T-Mobile

TABLE 1

Question 11 - Features/Settings	
WebCode	Response
TF6KA7	T-Mobile
UMXFKA	T-Mobile
UZMCL8	T-Mobile
V3PCKJ	T-Mobile
V8MVLH	TMobile
VFWK22	T-Mobile
VNNZQ6	T-Mobile
WKJPAV	T-Mobile
WMDDTR	T-Mobile
WUUUHF	T-Mobile
XMPFC6	TMobile
XMTWCN	T-Mobile
XX9QNG	T-Mobile
Y4U2D7	T Mobile
ZE9HK3	T-Mobile
ZNEHVP	T-MOBILE

Consensus Result: T-Mobile

Expected Response Explanation:

Several automated messages received from T-Mobile indicate that the service provider for 12023787266 is T-Mobile. These messages can be located at: /var/mobile/Library/SMS/sms.db

Expected Response Illustration:

Service Provider

5/11/2018 01:23 PM(UTC-4) Welcome to T-Mobile! Dial #BAL# to check your balances. Your T-Mobile number is 12023787266

TABLE 1

Question 12 - Features/Settings

Question 12: Provide the name (SSID) of the location this device was last connected to using Wi-Fi.

Manufacturer's Expected Response: Walmartwifi

WebCode	Response
22YJRM	Walmartwifi
2PK3JP	Walmartwifi
2UUKEC	Walmartwifi
42996J	Walmartwifi
4CQRKA	Walmartwifi
4N7HNL	Walmartwifi
6VXEL8	Walmartwifi
7W9GAR	Walmartwifi
7WNX6K	Walmartwifi
7YP3H6	Walmartwifi
88MVQY	Walmartwifi
94JJ86	Walmartwifi
94W9BG	Walmartwifi
9UUTMX	Walmartwifi
A2Q6XK	Walmartwifi
ATHB7D	Walmartwifi
B3XPLK	Walmartwifi
B4U49D	Walmartwifi
CEB8TH	Walmartwifi
CW7WPB	Walmartwifi
D2H6QF	Walmartwifi
DBKM2J	Walmartwifi
DPMTFN	Walmartwifi
DR6DZH	Walmartwifi
EZ2BMK	Walmartwifi
FA2K8F	00:41:D2:40:DD:CF
FML3XX	Walmartwifi
FV2JUE	Walmartwifi
FWCHNM	Walmartwifi
LVHNTTE	Walmartwifi
NQGLFN	Walmartwifi
PBMBAX	Walmartwifi
PFELHB	Walmartwifi
Q37ZWW	Walmart wifi
REWD8D	Walmartwifi
RWF8X3	Walmartwifi
TF6KA7	Walmartwifi

TABLE 1

Question 12 - Features/Settings	
WebCode	Response
UMXFKA	Walmartwifi
UZMCL8	Walmartwifi
V3PCKJ	Walmartwifi
V8MVLH	Walmartwifi
VFWK22	Walmartwifi
VNNZQ6	Walmartwifi
WKJPAV	Walmartwifi
WMDDTR	Walmartwifi
WUUUHF	Walmartwifi
XMPFC6	Walmartwifi
XMTWCN	Walmartwifi
XX9QNG	Walmartwifi
Y4U2D7	Walmartwifi
ZE9HK3	Walmartwifi
ZNEHVP	Walmartwifi

Consensus Result: Walmartwifi

Expected Response Explanation:

The service set identifier of the last location this device was connected to can be found within the com.apple.wifi.plist file which is located at: /var/preferences/SystemConfiguration/com.apple.wifi.plist

Expected Response Illustration:

SSID:

Name:	Walmartwifi
Description:	BSSID: 00:41:D2:40:DD:CF SSID: Walmartwifi
Type:	Wireless Network Last Connection
Origin:	
Timestamp:	5/24/2018 10:45 AM(UTC-4)

TABLE 1

Question 13 - Features/Settings

Question 13: Provide the phone number associated with this device.

Manufacturer's Expected Response: (202) 378-7266

WebCode	Response
22YJRM	12023787266
2PK3JP	+1 (202) 378-7266
2UUKEC	+1 (202) 378-7266
42996J	+12023787266
4CQRKA	1 (202) 378-7266
4N7HNL	+12023787266
6VXEL8	12023787266
7W9GAR	+1 (202) 378-7266
7WNX6K	+1 (202) 378-7266
7YP3H6	1-202-378-7266
88MVQY	+1 (202) 378-7266
94JJ86	+1 (202) 378-7266
94W9BG	(202)378-7266
9UUTMX	+1 (202) 378-7266
A2Q6XK	+1 (202) 378-7266
ATHB7D	+1 (202)378-7266
B3XPLK	+1 (202) 378-7266
B4U49D	2023787266
CEB8TH	+12023787266
CW7WPB	+1(202)378-7266
D2H6QF	+12023787266
DBKM2J	+1 (202) 378-7266
DPMTFN	+1 (202) 378-7266
DR6DZH	12023787266
EZ2BMK	+1 (202) 378-7266
FA2K8F	12023787266
FML3XX	202-378-7266
FV2JUE	(202) 378-7266
FWCHNM	+1 (202) 378-7266
LVHNT	202-378-7266
NQGLFN	+1 202-378-7266
PBMBAX	+1 (202) 378-7266
PFELHB	202-378-7266
Q37ZWW	+1 (202) 378-7266
REWD8D	+1 (202) 378-7266
RWF8X3	+1 (202) 378-7266
TF6KA7	+1 202-378-7266

TABLE 1

Question 13 - Features/Settings	
WebCode	Response
UMXFKA	+1 (202) 378-7266
UZMCL8	12023787266
V3PCKJ	+1 (202) 378-7266
V8MVLH	202-378-7266
VFWK22	1-202-378-7266
VNNZQ6	202-378-7266
WKJPAV	+1 (202) 378-7266
WMDDTR	1-202-378-7266
WUUUHF	202-378-7266
XMPFC6	+12023787266
XMTWCN	+1 (202) 378-7266
XX9QNG	+1 (202) 378-7266
Y4U2D7	+1 (202) 378-7266
ZE9HK3	(202) 378-7266
ZNEHVP	+1 (202)378-7266

Consensus Result: (202) 378-7266

Expected Response Explanation:

Mobile Station International Subscriber Directory Number (MSISDN) can be used to identify the mobile number of this device. It can be found within the apple.commcenter.plist file (offset 0x26E) which is located at: /var/wireless/Library/Preferences/com.apple.commcenter.plist

Expected Response Illustration:

MSISDN:

```
00000268 | DD 7B D2 E4 FC 5B 31 32 30 32 33 37 38 37 | .{...[12023787
00000276 | 32 36 36 33 41 C0 60 17 00 1A 18 F8 5C 2B | 2663A.`.....\+
00000284 | 31 32 30 32 33 37 38 37 32 36 36 5F 10 13 | 12023787266_..
```

Highlights [1 results]

#	Offset	Length	Value	Source
1	0x26E	0xB	MSISDN	/var/wireless/Library/Preferences/com.apple.commcenter.plist

TABLE 1

Question 14 - Application/Settings	
------------------------------------	--

Question 14: Based on the evidence, which two medications were prescribed to the user? Separate the medications with a comma (,)

Manufacturer's Expected Response: Celexa, Lexapro

WebCode	Response
22YJRM	Celexa, Lexapro
2PK3JP	Celexa, Lexapro
2UUKEC	Celexa, Lexapro
42996J	Lexapro, Celexa
4CQRKA	Celexa, Lexapro
4N7HNL	Celexa, Lexapro
6VXEL8	Celexa, Lexapro
7W9GAR	Celexa, Lexapro
7WNX6K	Celexa, Lexapro
7YP3H6	Celexa, Lexapro
88MVQY	Celexa, Lexapro
94JJ86	Celexa, Lexapro
94W9BG	Celexa, Lexapro
9UUTMX	Celexa, Lexapro
A2Q6XK	Celexa, Lexapro
ATHB7D	Celexa, Lexapro
B3XPLK	Celexa, Lexapro
B4U49D	Celexa, Lexapro
CEB8TH	Celexa, Lexapro
CW7WPB	Celexa, Lexapro
D2H6QF	Celexa, lexapro
DBKM2J	Lexapro, Celexa
DPMTFN	Celexa, Lexapro
DR6DZH	Celexa, Lexapro
EZ2BMK	Celexa, Lexapro
FA2K8F	Celexa, Lexapro
FML3XX	Celexa, Lexapro
FV2JUE	Celexa, Lexapro
FWCHNM	Celexa, Lexapro
LVHNTTE	Celexa, Lexapro
NQGLFN	Celexa, Lexapro
PBMBAX	Celexa, Lexapro
PFELHB	Celexa, Lexapro
Q37ZWW	Celexa, Lexapro
REWD8D	Celexa, Lexapro
RWF8X3	Celexa, Lexapro
TF6KA7	Celexa, Lexapro

TABLE 1

Question 14 - Application/Settings	
WebCode	Response
UMXFKA	Celexa, Lexapro
UZMCL8	Celexa, Lexapro
V3PCKJ	Celexa, Lexapro
V8MVLH	Celexa, Lexapro
VFWK22	Celexa, Lexapro
VNNZQ6	Celexa, Lexapro
WKJPAV	Celexa, Lexapro
WMDDTR	Celexa, Lexapro
WUUUHF	Celexa, Lexapro
XMPFC6	Celexa, Lexapro
XMTWCN	Celexa, Lexapro
XX9QNG	Celexa, Lexapro
Y4U2D7	Celexa, Lexapro
ZE9HK3	Celexa, Lexapro
ZNEHVP	CELEXA, LEXAPRO

Consensus Result: Celexa, Lexapro

Expected Response Explanation:

The names of the two medications were found in iOS Notes application. This application uses NoteStore.sqlite file to store all the data regarding each note saved on the device. NoteStore.sqlite file can be located at: /Applications/group.com.apple.notes/NoteStore.sqlite

Expected Response Illustration:

Note Title and Body:

Title	Body
Prescribed medicine by Dr. Shaw	Prescribed medicine by Dr. Shaw Take Celexa twice a day Take Lexapro daily

TABLE 1

Question 15 - Application/Settings	
------------------------------------	--

Question 15: What is the version of ExpediaBookings application installed on this device?

Manufacturer's Expected Response: 33.8.1

WebCode	Response
22YJRM	33.8.1
2PK3JP	33.8.1
2UUKEC	33.8.1
42996J	33.8.1
4CQRKA	33.8.1
4N7HNL	33.8.1
6VXEL8	33.8.1
7W9GAR	33.8.1
7WNX6K	33.8.1
7YP3H6	33.8.1
88MVQY	33.8.1
94JJ86	33.8.1
94W9BG	33.8.1
9UUTMX	33.8.1
A2Q6XK	33.8.1
ATHB7D	33.8.1
B3XPLK	33.8.1
B4U49D	33.8.1
CEB8TH	33.8.1
CW7WPB	33.8.1
D2H6QF	18.20 (3381)
DBKM2J	33.8.1
DPMTFN	33.8.1
DR6DZH	33.8.1
EZ2BMK	33.8.1
FA2K8F	33.8.1
FML3XX	33.8.1
FV2JUE	33.8.1
FWCHNM	33.8.1
LVHNTTE	33.8.1
NQGLFN	33.8.1
PBMBAX	33.8.1
PFELHB	33.8.1
Q37ZWW	33.8.1
REWD8D	33.8.1
RWF8X3	33.8.1
TF6KA7	18.20

TABLE 1

Question 15 - Application/Settings	
WebCode	Response
UMXFKA	33.8.1
UZMCL8	33.8.1
V3PCKJ	33.8.1
V8MVLH	33.8.1
VFWK22	33.8.1
VNNZQ6	33.8.1
WKJPAV	33.8.1
WMDDTR	33.8.1
WUUUHF	33.8.1
XMPFC6	33.8.1
XMTWCN	33.8.1
XX9QNG	33.8.1
Y4U2D7	33.8.1
ZE9HK3	33.8.1
ZNEHVP	33.8.1

Consensus Result: 33.8.1

Expected Response Explanation:

Information regarding installed applications can be found within the manifest.plist file.

Expected Response Illustration:

ExpediaBookings Version:

Name:	ExpediaBookings
Version:	33.8.1

TABLE 1

Question 16 - Application/Settings

Question 16: What is the version of the Skype application installed on this device?

Manufacturer's Expected Response: 8.21.0.7

WebCode	Response
22YJRM	8.21.0.7
2PK3JP	8.21.0.7
2UUKEC	8.21.0.7
42996J	Lexapro, Celexa
4CQRKA	8.21.0.7
4N7HNL	8.21.0.7
6VXEL8	8.21.0.7
7W9GAR	8.21.0.7
7WNX6K	8.21.0.7
7YP3H6	8.21.0.7
88MVQY	8.21.0.7
94JJ86	8.21.0.7
94W9BG	8.21.0.7
9UUTMX	8.21.0.7
A2Q6XK	8.21.0.7
ATHB7D	8.21.0.7
B3XPLK	8.21.0.7
B4U49D	8.21.0.7
CEB8TH	8.21.0.7
CW7WPB	8.21.0.7
D2H6QF	8.21.0.7
DBKM2J	Skype4life Ver. 8.21.0.7
DPMTFN	8.21.0.7
DR6DZH	8.21.0.7
EZ2BMK	8.21.0.7
FA2K8F	8.21.0.7
FML3XX	8.21.0.7
FV2JUE	8.21.0.7
FWCHNM	8.21.0.7
LVHNTTE	8.21.0.7
NQGLFN	8.21.0.7
PBMBAX	8.21.0.7
PFELHB	8.21.0.7
Q37ZWW	8.21.0.7
REWD8D	8.21.0.7
RWF8X3	8.21.0.7
TF6KA7	8.21.0.7

TABLE 1

Question 16 - Application/Settings	
WebCode	Response
UMXFKA	8.21.0.7
UZMCL8	8.21.0.7
V3PCKJ	8.21.0.7
V8MVLH	8.21.0.7
VFWK22	8.21.0.7
VNNZQ6	8.21.0.7
WKJPAV	8.21.0.7
WMDDTR	8.21.0.7
WUUUHF	8.21.0.7
XMPFC6	8.21.0.7
XMTWCN	8.21.0.7
XX9QNG	8.21.0.7
Y4U2D7	8.21.0.7
ZE9HK3	8.21.0.7
ZNEHVP	8.21.0.7

Consensus Result: 8.21.0.7

Expected Response Explanation:

Information regarding installed applications can be found within the manifest.plist file.

Expected Response Illustration:

Skype App Version:

Installed Application	
Name:	Skype4Life
Version:	8.21.0.7

TABLE 1

Question 17 - Application/Settings

Question 17: What is the user's Skype username? Provide the answer using the following format:

live:_____

Manufacturer's Expected Response: live:Thyne13

WebCode	Response
22YJRM	live:thyne13
2PK3JP	live:thyne13
2UUKEC	live:thyne13
42996J	live:thyne13
4CQRKA	live:thyne13
4N7HNL	thyne13
6VXEL8	live:thyne13
7W9GAR	thyne13
7WNX6K	live:thyne13
7YP3H6	live:/thyne13
88MVQY	live:thyne13
94JJ86	live:thyne13
94W9BG	live:thyne13
9UUTMX	live:thyne13
A2Q6XK	live:thyne13
ATHB7D	live: thyne13
B3XPLK	live:thyne13
B4U49D	live:thyne13
CEB8TH	live:thyne13
CW7WPB	Live:Thyne13
D2H6QF	live:thyne13
DBKM2J	live:thyne13
DPMTFN	live:thyne13
DR6DZH	live:thyne13
EZ2BMK	live:thyne13
FA2K8F	live:thyne13
FML3XX	live:thyne13
FV2JUE	live:thyne13
FWCHNM	live:thyne13
LVHNTTE	live:thyne13
NQGLFN	live:thyne13
PBMBAX	live:thyne13
PFELHB	live:thyne13
Q37ZWW	live:thyne13
REWD8D	live:thyne13
RWF8X3	live:thyne13
TF6KA7	live:thyne13

TABLE 1

Question 17 - Application/Settings	
WebCode	Response
UMXFKA	live:thyne13
UZMCL8	live:thyne13
V3PCKJ	live: thyne13
V8MVLH	live.thyne13
VFWK22	live:thyne13
VNNZQ6	live:thyne13
WKJPAV	live:thyne13
WMDDTR	live:thyne13
WUUUHF	live:thyne13
XMPFC6	live:thyne13
XMTWCN	live:thyne13
XX9QNG	thyne13
Y4U2D7	live:thyne13
ZE9HK3	live:thyne13
ZNEHVP	live:thyne13

Consensus Result: live:Thyne13

Expected Response Explanation:

The user account information for the Skype application is stored in the main.db which can be located at: /Applications/com.skype.skype/Library/Application Support/Skype4LifeSlimCore/live#3athyne13/main.db

Expected Response Illustration:

Skype Username

Username	Service Type
live:thyne13	Skype

TABLE 1

Question 18 - Application/Settings

Question 18: What is the user's Facebook login email ID?

Manufacturer's Expected Response: mthyne13@gmail.com

WebCode	Response
22YJRM	mthyne13@gmail.com
2PK3JP	mthyne13@gmail.com
2UUKEC	mthyne13@gmail.com
42996J	mthyne13@gmail.com
4CQRKA	mthyne13@gmail.com
4N7HNL	mthyne13@gmail.com
6VXEL8	mthyne13@gmail.com
7W9GAR	mthyne13@gmail.com
7WNX6K	mthyne13@gmail.com
7YP3H6	mthyne13@gmail.com
88MVQY	mthyne13@gmail.com
94JJ86	mthyne13@gmail.com
94W9BG	mthyne13@gmail.com
9UUTMX	Email= mthyne13@gmail.com, ID= 100026066000921
A2Q6XK	mthyne13@gmail.com
ATHB7D	mthyne13@gmail.com
B3XPLK	mthyne13@gmail.com
B4U49D	mthyne13@gmail.com
CEB8TH	mthyne13@gmail.com
CW7WPB	Mthyne13@gmail.com
D2H6QF	mthyne13@gmail.com
DBKM2J	mthyne13@gmail.com
DPMTFN	mthyne13@gmail.com
DR6DZH	mthyne13@gmail.com 100026066000921
EZ2BMK	mthyne13@gmail.com
FA2K8F	mthyne13@gmail.com
FML3XX	mthyne13@gmail.com
FV2JUE	mthyne13@gmail.com
FWCHNM	mthyne13@gmail.com
LVHNT	mthyne13@gmail.com
NQGLFN	mthyne13@gmail.com
PBMBAX	mthyne13@gmail.com
PFELHB	Mthyne13@gmail.com
Q37ZWW	mthyne13@smail.com
REWD8D	mthyne13@gmail.com
RWF8X3	100026066000921
TF6KA7	mthyne13@gmail.com

TABLE 1

Question 18 - Application/Settings	
WebCode	Response
UMXFKA	mthyne13@gmail.com
UZMCL8	mthyne13@gmail.com
V3PCKJ	mthyne13@gmail.com
V8MVLH	mthyne13@gmail.com
VFWK22	mthyne13@gmail.com
VNNZQ6	mthyne13@gmail.com
WKJPAV	mthyne13@gmail.com
WMDDTR	mthyne13@gmail.com
WUUUHF	mthyne13@gmail.com
XMPFC6	mthyne13@gmail.com
XMTWCN	Facebook ID 100026066000921 mthyne13@gmail.com
XX9QNG	mthyne13@gmail.com
Y4U2D7	mthyne13@gmail.com
ZE9HK3	mthyne13@gmail.com
ZNEHVP	mthyne13@gmail.com

Consensus Result: mthyne13@gmail.com

Expected Response Explanation:

Information about the user account associated with the Facebook application is stored in the com.facebook.Facebook.plist (offset 0x20771) file which can be located at:
/Applications/com.facebook.Facebook/Library/Preferences/com.facebook.Facebook.plist

Expected Response Illustration:

Facebook Login ID:

```
Facebook Id 100026066000921
mthyne13@gmail.com
```

TABLE 1

Question 19 - Application/Settings

Question 19: What is the user's Facebook password?

Manufacturer's Expected Response: Polarbear13

WebCode	Response
22YJRM	polarbear13
2PK3JP	polarbear13
2UUKEC	polarbear13
42996J	polarbear13
4CQRKA	polarbear13
4N7HNL	it is not shown (encrypted)
6VXEL8	polarbear13
7W9GAR	polarbear13
7WNX6K	polarbear13
7YP3H6	polarbear13
88MVQY	polarbear13
94JJ86	polarbear13
94W9BG	polarbear13
9UUTMX	polarbear13
A2Q6XK	polarbear13
ATHB7D	polarbear13
B3XPLK	polarbear13
B4U49D	polarbear13
CEB8TH	polarbear13
CW7WPB	polarbear13
D2H6QF	polarbear13
DBKM2J	polarbear13
DPMTFN	polarbear13
DR6DZH	polarbear13
EZ2BMK	polarbear13
FA2K8F	polarbear13
FML3XX	polarbear13
FV2JUE	polarbear13
FWCHNM	polarbear13
LVHNTTE	polarbear13
NQGLFN	polarbear13
PBMBAX	polarbear13
PFELHB	Polarbear13
Q37ZWW	polarbear13
REWD8D	polarbear13
RWF8X3	polarbear13
TF6KA7	polarbear13

TABLE 1

Question 19 - Application/Settings	
WebCode	Response
UMXFKA	polarbear13
UZMCL8	polarbear13
V3PCKJ	polarbear13
V8MVLH	polarbear13
VFWK22	polarbear13
VNNZQ6	polarbear13
WKJPAV	polarbear13
WMDDTR	polarbear13
WUUUHF	polarbear13
XMPFC6	polarbear13
XMTWCN	polarbear13
XX9QNG	polarbear13
Y4U2D7	polarbear13
ZE9HK3	polarbear13
ZNEHVP	polarbear13

Consensus Result: Polarbear13

Expected Response Explanation:

Account passwords are stored in the keychain-backup.plist file which can be located at: /var/Keychains/keychain-backup.plist

Expected Response Illustration:

Facebook account password:



TABLE 1

Question 20 - Application/Settings	
------------------------------------	--

Question 20: Based on the evidence, what is the home address for Annie Fao? Provide the Street, City, State, and Zip code. (Ex: 1234 Adams St., Chester, FL 10056)

Manufacturer's Expected Response: 16444 Atlanta Drive, Fairfax, VA 20091

WebCode	Response
22YJRM	16444 Atlanta Drive, Fairfax, VA 20091
2PK3JP	16444 Atlanta Drive, Fairfax, VA 20091
2UUKEC	16444 Atlanta Drive, Fairfax, VA 20091
42996J	16444 Atlanta Drive, Fairfax, VA 20091
4CQRKA	16444 Atlanta Drive, Fairfax, VA 20091
4N7HNL	16444 Atlanta Drive, Fairfax, VA 20091
6VXEL8	16444 Atlanta Drive, Fairfax, VA 20091
7W9GAR	Annie Fao's home address 16444 Atlanta Drive Fairfax, VA 20091
7WNX6K	16444 Atlanta Drive, Fairfax, VA 20091
7YP3H6	16444 Atlanta Drive Fairfax, VA 20091
88MVQY	16444 Atlanta Drive, Fairfax, VA 20091
94JJ86	16444 Atlanta Drive, Fairfax, VA 20091
94W9BG	16444 Atlanta Dr., Fairfax VA 20091
9UUTMX	16444 Atlanta Drive, Fairfax, VA 20091
A2Q6XK	16444 Atlanta Drive, Fairfax, VA 20091
ATHB7D	16444 Atlanta Drive Fairfax, VA 20091
B3XPLK	16444 Atlanta Drive, Fairfax, Virginia, VA 20091
B4U49D	16444 Atlanta Drive, Fairfax, VA 20091
CEB8TH	16444 Atlanta Drive, Fairfax, VA 20091
CW7WPB	16444 Atlanta Drive, Fairfax, VA 20091
D2H6QF	16444 Atlanta Drive, Fairfax, VA 20091
DBKM2J	16444 Atlanta Drive, Fairfax, VA 20091
DPMTFN	16444 Atlanta Drive, Fairfax, VA 20091
DR6DZH	16444 Atlanta Drive, Fairfax, VA 20091
EZ2BMK	16444 Atlanta Drive, Fairfax, VA 20091
FA2K8F	16444 Atlanta Drive Fairfax, VA 20091
FML3XX	16444 Atlanta Drive, Fairfax, VA 20091
FV2JUE	16444 Atlanta Drive, Fairfax, VA 20091
FWCHNM	16444 Atlanta Drive Fairfax, VA 20091
LVHNTTE	16444 Atlanta Drive, Fairfax, VA 20091
NQGLFN	16444 Atlanta Drive, Fairfax, VA, 20091
PBMBAX	16444 Atlanta Drive, Fairfax, VA 20091
PFELHB	16444 Atlanta Drive Fairfax, VA 20091
Q37ZWW	16444 Atlanta Drive, Fairfax, VA 20091
REWD8D	16444 Atlanta Drive Fairfax, VA 20091
RWF8X3	16444 Atlanta Drive Fairfax, VA 20091
TF6KA7	16444 Atlanta Drive, Fairfax, VA 20091

TABLE 1

Question 20 - Application/Settings	
WebCode	Response
UMXFKA	16444 Atlanta Drive, Fairfax, VA 20091
UZMCL8	16444 Atlanta Drive Fairfax, VA 20091
V3PCKJ	16444 Atlanta Drive, Fairfax, VA 20091
V8MVLH	16444 Atlanta Drive Fairfax, VA 20091
VFWK22	16444 Atlanta Dr., Fairfax VA 20091
VNNZQ6	16444 Atlanta Drive Fairfax, VA 20091
WKJPAV	16444 Atlanta Drive, Fairfax, VA 20091
WMDDTR	16444 Atlanta Drive, Fairfax, VA 20091
WUUUHF	16444 Atlanta Drive, Fairfax, VA 20091
XMPFC6	16444 Atlanta Drive, Fairfax, VA 20091
XMTWCN	16444 Atlanta Drive, Fairfax, VA, 20091
XX9QNG	16444 Atlanta Drive, Fairfax, VA 20091
Y4U2D7	16444 Atlanta Drive Fairfax, VA 20091
ZE9HK3	16444 Atlanta Dr., Fairfax VA 20091
ZNEHVP	16444 Atlanta Drive, Fairfax, VA 20091

Consensus Result: 16444 Atlanta Drive, Fairfax, VA 20091

Expected Response Explanation:

The home address of a Annie Fao was found in iOS Notes application. This application uses NoteStore.sqlite database to store all the data regarding each note saved on the device. NoteStore.sqlite file can be located at /Applications/group.com.apple.notes/NoteStore.sqlite

Expected Response Illustration:

Note Title and Body:

Title	Body
Annie Fao's home address	Annie Fao's home address 16444 Atlanta Drive Fairfax, VA 20091

TABLE 1

Question 21 - Application/Settings

Question 21: Provide the longitude and latitude of the last place viewed using Google Maps Application.
Answer using the following format: Longitude: _____, Latitude: _____

Manufacturer's Expected Response: Longitude: -77.3967717728168, Latitude:
 38.8548381516278

WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
22YJRM	Longitude: 38.854838, Latitude: -77.396772	
2PK3JP	Longitude: 38.854838, Latitude:-77.396772	
2UUKEC	Longitude: 38.854838, Latitude: -77.396772	
42996J	Longitude: -77.396772, Latitude: 38.854838	
4CQRKA	Longitude: 38.854838, Latitude: -77.396772	
4N7HNL	Longitude: 38.854838, Latitude:-77.396772	
6VXEL8	Longitude: -77.396772, Latitude: 38.854838	
7W9GAR	(38.854838, -77.396772)	
7WNX6K	Longitude: -77.39677177281682, Latitude: 38.85483815162776	
7YP3H6	Longitude: 38.854838, Latitude: -77.396772	
88MVQY	Longitude:38.854838, Latitude: -77.396772	
94JJ86	Longitude: -77.39677177728168, Latitude: 38.8548381516278	
94W9BG	Longitude: -77.396772, Latitude: 38.854838	
9UUTMX	Longitude: -77.396772, Latitude: 38.854838	
A2Q6XK	Longitude:-77.396772, Latitude:38.854838	
ATHB7D	Longitude: -77.39677177281682, Latitude: 38.85483815162776	
B3XPLK	Longitude: -77.396772, Latitude: 38.854838	
B4U49D	Longitude: -77.396772, Latitude: 38.854838	
CEB8TH	Longitude: 38.854838, Latitude: -77.396772	
CW7WPB	Longitude:-77.396772, Latitude:38.854838	
D2H6QF	Longitude: -77.3967717728168, Latitude: 38.8548381516278	
DBKM2J	Longitude: 38.854838, Latitude: 77.396772	
DPMTFN	Longitude: -77.396772 Latitude: 38.85483.	
DR6DZH	Longitude: -77.2614 Latitude: 38.8721	
EZ2BMK	Longitude: -77.3967717728168, Latitude: 38.8548381516278	
FA2K8F	Longitude:-77.396772, Latitude:38.854838	
FML3XX	Longitude: -77.396772, Latitude: 38.854838	
FV2JUE	Longitude: 38.854838, Latitude: -77.396772	
FWCHNM	Longitude:38.854838, Latitude:-77.396772	
LVHNT	38.854838, -77.396772	
NQGLFN	Longitude: -77.396772, Latitude: 38.8548388	
PBMBAX	Longitude: -77.3967717728168, Latitude: 38.8548381516278	
PFELHB	Longitude: 38.854838, Latitude: -77.396772	
Q37ZWW	Longitude: 38854838, Latitude: 77396772	
REWD8D	Longitude: -77.396772, Latitude: 38.854838	
RWF8X3	Longitude: 38.854838, Latitude: -77.396772	
TF6KA7	Longitude: -77.3967717728168, Latitude: 38.8548381516278	

TABLE 1

Question 21 - Application/Settings		
WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
UMXFKA	Longitude: -77.396772, Latitude: 38.854838	
UZMCL8	Longitude: 38.854838, Latitude: -77.396772	
V3PCKJ	Longitude: -77.396772, Latitude: 38.854838	
V8MVLH	Longitude: -77.396772, Latitude: 38.854838	
VFWK22	Longitude: 38.854838, Latitude: -77.396772	
VNNZQ6	Longitude: -77.396772, Latitude: 38.854838	
WKJPAV	Longitude: -77.3967717728168, Latitude: 38.8548381516278	
WMDDTR	Longitude: -77.396772, Latitude: 38.854838	
WUUUHF	Longitude: -77.396772, Latitude: 38.854838	
XMPFC6	Longitude: 38.854838, Latitude: -77.396772	
XMTWCN	Longitude: -77.396772, Latitude: 38.854838	
XX9QNG	-77.396772, 38.854838	
Y4U2D7	Longitude: 38.854838, Latitude: -77.396772	
ZE9HK3	Longitude: 38.854838, Latitude:-77.396772	
ZNEHVP	LONGITUDE:-77.396772, LATITUDE:38.854838	

Consensus Result: Consensus was not achieved for this question primarily because approximately half of the participants labeled GPS coordinates opposite to expected format. These participants reported the expected latitude values as longitude and longitude values as latitude.

Expected Response Explanation:

The GPS coordinates of the last location viewed are stored within the com.google.Maps.plist file which can be located at: /Applications/com.google.Maps/Library/Preferences/com.google.Maps.plist

Expected Response Illustration:

GPS Coordinates:

Offset	Length	Value
0x1705	0x8	Coordinate.Longitude: -77.3967717728168
0x172B	0x8	Coordinate.Latitude: 38.8548381516278
0x1748	0x8	Location.TimeStamp: 5/24/2018 10:45 AM(UTC-4)

Timestamp	Position	Category
5/24/2018 10:45 AM(UTC-4)	(38.854838, -77.396772)	Google Maps

TABLE 1

Question 22 - Application/Settings

Question 22: What was the last phrase searched using the Safari search engine?

Manufacturer's Expected Response: ways to commit suicide

WebCode	Response
22YJRM	ways to commit suicide
2PK3JP	ways to commit suicide
2UUKEC	ways to commit suicide
42996J	ways to commit suicide
4CQRKA	ways to commit suicide
4N7HNL	ways to commit suicide
6VXEL8	ways to commit suicide
7W9GAR	ways to commit suicide
7WNX6K	ways to commit suicide
7YP3H6	ways to commit suicide
88MVQY	Ways to commit suicide
94JJ86	ways to commit suicide
94W9BG	ways to commit suicide
9UUTMX	ways to commit suicide
A2Q6XK	ways to commit suicide
ATHB7D	ways to commit suicide
B3XPLK	ways to commit suicide
B4U49D	ways to commit suicide
CEB8TH	ways to commit suicide
CW7WPB	ways to commit suicide
D2H6QF	ways to commit suicide
DBKM2J	Ways to commit suicide.
DPMTFN	"ways to commit suicide"
DR6DZH	ways to commit suicide
EZ2BMK	ways to commit suicide
FA2K8F	Ways to commit suicide
FML3XX	ways to commit suicide
FV2JUE	ways to commit suicide
FWCHNM	ways to commit suicide
LVHNT	ways to commit suicide
NQGLFN	ways to commit suicide
PBMBAX	ways to commit suicide
PFELHB	ways to commit suicide
Q37ZWW	ways to commit suicide
REWD8D	ways to commit suicide
RWF8X3	ways to commit suicide
TF6KA7	ways to commit suicide

TABLE 1

Question 22 - Application/Settings	
WebCode	Response
UMXFKA	ways to commit suicide
UZMCL8	Ways to commit suicide
V3PCKJ	ways to commit suicide
V8MVLH	ways to commit suicide
VFWK22	ways to commit suicide
VNNZQ6	ways to commit suicide
WKJPAV	ways to commit suicide
WMDDTR	ways to commit suicide
WUUUHF	ways to commit suicide
XMPFC6	ways to commit suicide
XMTWCN	"ways to commit suicide"
XX9QNG	ways to commit suicide
Y4U2D7	ways to commit suicide
ZE9HK3	ways to commit suicide
ZNEHVP	ways to commit suicide

Consensus Result: ways to commit suicide

Expected Response Explanation:

The search history using Safari search engine is stored within the History database which can be located at: /Applications/com.apple.mobilesafari/Library/Safari/History.db

Expected Response Illustration:

Last term searched using Safari:

Searched Item	
Timestamp:	5/23/2018 11:33 AM(UTC-4)
Source:	Safari
Value:	ways to commit suicide

TABLE 1

Question 23 - Application/Settings

Question 23: Provide the email ID which is associated with the user's iCloud account.

Manufacturer's Expected Response: thyne13@icloud.com

WebCode	Response
22YJRM	thyne13@icloud.com
2PK3JP	thyne13@icloud.com
2UUKEC	thyne13@icloud.com
42996J	thyne13@icloud.com
4CQRKA	thyne13@icloud.com
4N7HNL	thyne13@icloud.com
6VXEL8	thyne13@icloud.com
7W9GAR	thyne13@icloud.com
7WNX6K	thyne13@icloud.com
7YP3H6	thyne13@icloud.com
88MVQY	thyne13@icloud.com
94JJ86	thyne13@icloud.com
94W9BG	thyne13@icloud.com
9UUTMX	thyne13@icloud.com
A2Q6XK	thyne13
ATHB7D	thyne13@icloud.com
B3XPLK	thyne13@icloud.com
B4U49D	thyne13@icloud.com
CEB8TH	thyne13@icloud.com
CW7WPB	thyne13@icloud.com
D2H6QF	thyne13@icloud.com
DBKM2J	thyne13@icloud.com
DPMTFN	thyne13@icloud.com
DR6DZH	thyne13@icloud.com
EZ2BMK	thyne13@icloud.com
FA2K8F	thyne13@icloud.com
FML3XX	thyne13@icloud.com
FV2JUE	thyne13@icloud.com
FWCHNM	thyne13@icloud.com
LVHNTTE	thyne13@icloud.com
NQGLFN	thyne13@icloud.com
PBMBAX	thyne13@icloud.com
PFELHB	thyne13@icloud.com
Q37ZWW	thyne13@icloud.com
REWD8D	thyne13@icloud.com
RWF8X3	thyne13@icloud.com
TF6KA7	thyne13@icloud.com

TABLE 1

Question 23 - Application/Settings	
WebCode	Response
UMXFKA	thyne13@icloud.com
UZMCL8	thyne13@icloud.com
V3PCKJ	thyne13@icloud.com
V8MVLH	thyne13@icloud.com
VFWK22	thyne13@icloud.com
VNNZQ6	thyne13@icloud.com
WKJPAV	thyne13@icloud.com
WMDDTR	thyne13@icloud.com
WUUUHF	thyne13@icloud.com
XMPFC6	thyne13@icloud.com
XMTWCN	thyne13@icloud.com
XX9QNG	thyne13@icloud.com
Y4U2D7	thyne13@icloud.com
ZE9HK3	thyne13@icloud.com
ZNEHVP	thyne13@icloud.com

Consensus Result: thyne13@icloud.com

Expected Response Explanation:

Information about the email ID associated with the iCloud account is stored in the com.apple.homesharing.plist file which can be located at: /var/mobile/Library/Preferences/com.apple.homesharing.plist

Expected Response Illustration:

AppleID:

Account	Username
com.apple.accounts.accountsd	thyne13@icloud.com

```
10 12 74 68 79 6E 65 31 33 40 69 63 | ..thyne13@ic
6C 6F 75 64 2E 63 6F 6D 23 41 C0 64 | loud.com#A.d
```

TABLE 1

Question 24 - Application/Settings

Question 24: What is the password of the iCloud account on this device?

Manufacturer's Expected Response: 2019Graduate

WebCode	Response
22YJRM	2019Graduate
2PK3JP	2019Graduate
2UUKEC	2019Graduate
42996J	2019Graduate
4CQRKA	2019Graduate
4N7HNL	2019Graduate
6VXEL8	2019Graduate
7W9GAR	2019Graduate
7WNX6K	2019Graduate
7YP3H6	2019Graduate
88MVQY	2019Graduate
94JJ86	2019Graduate
94W9BG	2019Graduate
9UUTMX	2019Graduate
A2Q6XK	2019Graduate
ATHB7D	2019Graduate
B3XPLK	2019Graduate
B4U49D	2019Graduate
CEB8TH	2019Graduate
CW7WPB	2019Graduate
D2H6QF	2019Graduate
DBKM2J	2019Graduate
DPMTFN	2019Graduate
DR6DZH	2019Graduate
EZ2BMK	2019Graduate
FA2K8F	2019Graduate
FML3XX	2019Graduate
FV2JUE	2019Graduate
FWCHNM	2019Graduate
LVHNTTE	2019Graduate
NQGLFN	2019Graduate
PBMBAX	2019Graduate
PFELHB	2019Graduate
Q37ZWW	2019Graduate
REWD8D	2019Graduate
RWF8X3	2019Graduate
TF6KA7	2019Graduate

TABLE 1

Question 24 - Application/Settings	
WebCode	Response
UMXFKA	2019Graduate
UZMCL8	2019Graduate
V3PCKJ	2019Graduate
V8MVLH	2019Graduate
VFWK22	2019Graduate
VNNZQ6	2019Graduate
WKJPAV	2019Graduate
WMDDTR	2019Graduate
WUUUHF	2019Graduate
XMPFC6	2019Graduate
XMTWCN	2019Graduate
XX9QNG	2019Graduate
Y4U2D7	2019Graduate
ZE9HK3	2019Graduate
ZNEHVP	2019Graduate

Consensus Result: 2019Graduate

Expected Response Explanation:

Account passwords are stored in the keychain-backup.plist file which can be located at:
/var/Keychains/keychain-backup.plist

Expected Response Illustration:

iCloud Account Password:

Password	
Access group:	com.apple.cfnetwork
Account:	thyne13@icloud.com
Data:	2019Graduate

TABLE 1

Question 25 - Communication

Question 25: How many voicemails were received from +1 571-484-0504?

Manufacturer's Expected Response: Two (2)

WebCode	Response
22YJRM	2
2PK3JP	2
2UUKEC	2
42996J	2
4CQRKA	2
4N7HNL	2
6VXEL8	2
7W9GAR	2
7WNX6K	2
7YP3H6	2
88MVQY	2
94JJ86	Two
94W9BG	2
9UUTMX	2
A2Q6XK	2
ATHB7D	2
B3XPLK	2
B4U49D	2
CEB8TH	2
CW7WPB	2
D2H6QF	2
DBKM2J	Two.
DPMTFN	2
DR6DZH	Two (2)
EZ2BMK	2
FA2K8F	2
FML3XX	2
FV2JUE	2
FWCHNM	2
LVHNTTE	2
NQGLFN	2
PBMBAX	2
PFELHB	2
Q37ZWW	2
REWD8D	2
RWF8X3	2
TF6KA7	2

TABLE 1

Question 25 - Communication	
WebCode	Response
UMXFKA	2
UZMCL8	2
V3PCKJ	2
V8MVLH	2
VFWK22	2
VNNZQ6	2
WKJPAV	2
WMDDTR	2
WUUUHF	2
XMPFC6	Two (2)
XMTWCN	2
XX9QNG	2
Y4U2D7	2
ZE9HK3	2
ZNEHVP	2

Consensus Result: Two (2)

Expected Response Explanation:

There were a total of two voicemails received from +1 571-484-0504. Information about voicemails received is stored in the voicemail.db which can be located at: /var/mobile/Library/Voicemail/voicemail.db

Expected Response Illustration:

Voicemails:

voicemail.db

	date	sender	duration
1	1526994299	+15714840504	10
2	1527168709	+15714840504	16

TABLE 1

Question 26 - Communication

Question 26: Other than iMessages, which 3rd party chat application did the user primarily use to send and receive messages from +1 571-484-0504?

Manufacturer's Expected Response: WhatsApp

WebCode	Response
22YJRM	WhatsApp
2PK3JP	WhatsApp
2UUKEC	WhatsApp
42996J	Whatsapp
4CQRKA	WhatsApp
4N7HNL	WhatsApp
6VXEL8	WhatsApp
7W9GAR	Whatsapp
7WNX6K	WhatsApp
7YP3H6	Whatsapp
88MVQY	WhatsApp
94JJ86	WhatsApp
94W9BG	WhatsApp
9UUTMX	WhatsApp
A2Q6XK	WhatsApp
ATHB7D	WhatsApp
B3XPLK	Whatsapp
B4U49D	WhatsApp
CEB8TH	WhatsApp
CW7WPB	WhatsApp
D2H6QF	WhatsApp
DBKM2J	Whatsapp
DPMTFN	WhatsApp
DR6DZH	WhatsApp
EZ2BMK	WhatsApp
FA2K8F	WhatsApp
FML3XX	WhatsApp
FV2JUE	WhatsApp
FWCHNM	WhatsApp
LVHNTTE	WhatsApp
NQGLFN	WhatsApp
PBMBAX	WhatsApp
PFELHB	WhatsApp
Q37ZWW	whatsapp
REWD8D	whatsapp
RWF8X3	WhatsApp
TF6KA7	WhatsApp

TABLE 1

Question 26 - Communication	
WebCode	Response
UMXFKA	WhatsApp
UZMCL8	Whatsapp
V3PCKJ	WhatsApp
V8MVLH	Whats App
VFWK22	WhatsApp
VNNZQ6	WhatsApp
WKJPAV	WhatsApp
WMDDTR	WhatsApp
WUUUHF	WhatsApp
XMPFC6	WhatsApp
XMTWCN	WhatsApp
XX9QNG	WhatsApp
Y4U2D7	WhatsApp
ZE9HK3	Whatsapp
ZNEHVP	WHATSAPP

Consensus Result: WhatsApp

Expected Response Explanation:

Besides iMessages, the WhatsApp application was the primary source used to communicate with a Annie Fao at +15714840504.

Expected Response Illustration:

Primary 3rd Party Application Used:

Participants	Source
+12023787266 (owner) +15714840504 Annie Fao	iMessage: +12023787266
12023787266@s.whatsapp.net Matthew Thy 15714840504@s.whatsapp.net Annie Fao	WhatsApp

TABLE 1

Question 27 - Communication

Question 27: To whom was the last phone call placed using this device? Provide the first and last name.
(First Last)

Manufacturer's Expected Response: Annie Fao

WebCode	Response
22YJRM	Annie Fao
2PK3JP	Annie Fao
2UUKEC	Annie Fao
42996J	Annie Fao
4CQRKA	Annie Fao
4N7HNL	Annie Fao
6VXEL8	Annie Fao
7W9GAR	Fao Annie
7WNX6K	Annie Fao
7YP3H6	Annie Fao
88MVQY	Annie Fao
94JJ86	Annie Fao
94W9BG	Annie Fao
9UUTMX	Annie Fao
A2Q6XK	Annie Fao
ATHB7D	Annie Fao
B3XPLK	Fao, Annie
B4U49D	Annie Fao
CEB8TH	Annie Fao
CW7WPB	Annie Fao
D2H6QF	Annie Fao
DBKM2J	Annie Fao
DPMTFN	Annie Fao
DR6DZH	Annie Fao
EZ2BMK	Annie Fao
FA2K8F	Annie Fao
FML3XX	Annie Fao
FV2JUE	Annie Fao
FWCHNM	Annie Fao
LVHNTTE	Annie Fao
NQGLFN	Annie Fao
PBMBAX	Annie Fao
PFELHB	Annie Fao
Q37ZWW	Annie Fao
REWD8D	Annie Fao
RWF8X3	Annie Fao
TF6KA7	Annie Fao

TABLE 1

Question 27 - Communication	
WebCode	Response
UMXFKA	Annie Fao
UZMCL8	Annie Fao
V3PCKJ	Annie Fao
V8MVLH	Annie Fao
VFWK22	Annie Fao
VNNZQ6	Annie Fao
WKJPAV	Annie Fao
WMDDTR	Annie Fao
WUUUHF	Annie Fao
XMPFC6	Annie Fao
XMTWCN	Annie Fao
XX9QNG	Annie Fao
Y4U2D7	Annie Fao
ZE9HK3	Annie Fao
ZNEHVP	ANNIE FAO

Consensus Result: Annie Fao

Expected Response Explanation:

The call history for this device is stored in the CallHistory.storedata file which can be located at: /var/mobile/Library/CallHistoryDB/CallHistory.storedata

Expected Response Illustration:

Last Outgoing Call:

Parties	Timestamp	Duration	Type	Source
To: +15714840504 Annie Fao	5/24/2018 12:47 PM(UTC-4)	00:08:06	Outgoing	FaceTime

TABLE 1

Question 28 - Communication

Question 28: What was the type of the last outgoing call placed using this device? Choose one of the following: Voice call, FaceTime

Manufacturer's Expected Response: FaceTime

WebCode	Response
22YJRM	FaceTime
2PK3JP	FaceTime
2UUKEC	FaceTime
42996J	Facetime
4CQRKA	FaceTime
4N7HNL	Voice Call
6VXEL8	FaceTime
7W9GAR	Video, Face Time.
7WNX6K	FaceTime
7YP3H6	Facetime
88MVQY	FaceTime
94JJ86	FaceTime
94W9BG	FaceTime
9UUTMX	FaceTime
A2Q6XK	FaceTime
ATHB7D	Face Time
B3XPLK	FaceTime
B4U49D	FaceTime
CEB8TH	FaceTime
CW7WPB	FaceTime
D2H6QF	FaceTime
DBKM2J	Facetime
DPMTFN	Facetime
DR6DZH	FaceTime
EZ2BMK	FaceTime
FA2K8F	FaceTime
FML3XX	FaceTime
FV2JUE	FaceTime
FWCHNM	FaceTime
LVHNTTE	FaceTime
NQGLFN	FaceTime
PBMBAX	FaceTime
PFELHB	Facetime
Q37ZWW	FaceTime
REWD8D	FaceTime
RWF8X3	FaceTime
TF6KA7	FaceTime

TABLE 1

Question 28 - Communication	
WebCode	Response
UMXFKA	FaceTime
UZMCL8	Face Time
V3PCKJ	FaceTime
V8MVLH	FaceTime
VFWK22	FaceTime
VNNZQ6	FaceTime
WKJPAV	FaceTime
WMDDTR	FaceTime
WUUUHF	Facetime
XMPFC6	FaceTime
XMTWCN	FaceTime
XX9QNG	FaceTime
Y4U2D7	FaceTime
ZE9HK3	FaceTime
ZNEHVP	FACETIME

Consensus Result: FaceTime

Expected Response Explanation:

The last outgoing call placed was FaceTime (video call) on 5/24/2018 at 12:47 PM(UTC-4). The call history for this device is stored in the CallHistory.storedata file which can be located at:
 /var/mobile/Library/CallHistoryDB/CallHistory.storedata

Expected Response Illustration:

Last Outgoing Call:

Parties	Timestamp	Duration	Type	Source
To: +15714840504 Annie Fao	5/24/2018 12:47 PM(UTC-4)	00:08:06	Outgoing	FaceTime

TABLE 1

Question 29 - Communication

Question 29: What is the duration of the last outgoing (audio or video) call? Answer using the following format: hh:mm:ss

Manufacturer's Expected Response: 00:08:06

WebCode	Response
22YJRM	00:08:06
2PK3JP	00:08:06
2UUKEC	00:08:06
42996J	00:08:06
4CQRKA	00:08:06
4N7HNL	00:08:06
6VXEL8	00:08:06
7W9GAR	00:08:06
7WNX6K	00:08:06
7YP3H6	00:08:06
88MVQY	00:08:06
94JJ86	00:08:06
94W9BG	00:08:06
9UUTMX	00:08:06
A2Q6XK	00:08:06
ATHB7D	00:08:07
B3XPLK	00:08:07
B4U49D	00:08:06
CEB8TH	00:08:06
CW7WPB	00:08:06
D2H6QF	00:08:06
DBKM2J	00:08:06
DPMTFN	00:08:06
DR6DZH	00:08:06
EZ2BMK	00:08:06
FA2K8F	00:08:06
FML3XX	00:08:06
FV2JUE	00:08:06
FWCHNM	00:08:06
LVHNTTE	00:08:06
NQGLFN	00:08:06
PBMBAX	00:08:06
PFELHB	00:08:06
Q37ZWW	00:08:06
REWD8D	00:08:06
RWF8X3	00:08:06
TF6KA7	00:08:06

TABLE 1

Question 29 - Communication	
WebCode	Response
UMXFKA	00:08:06
UZMCL8	00:08:06
V3PCKJ	00:08:06
V8MVLH	00:08:06
VFWK22	00:08:06
VNNZQ6	00:08:06
WKJPAV	00:08:06
WMDDTR	00:08:06
WUUUHF	00:08:06
XMPFC6	00:08:06
XMTWCN	The duration is 00:08:06 or 00:08:07 if rounded up.
XX9QNG	00:08:06
Y4U2D7	00:08:06
ZE9HK3	00:08:06
ZNEHVP	00:08:06

Consensus Result: 00:08:06

Expected Response Explanation:

The call history for this device is stored in the CallHistory.storedata file which can be located at: /var/mobile/Library/CallHistoryDB/CallHistory.storedata

Expected Response Illustration:

Call Duration:

Parties	Timestamp	Duration	Type	Source
To: +15714840504 Annie Fao	5/24/2018 12:47 PM(UTC-4)	00:08:06	Outgoing	FaceTime

TABLE 1

Question 30 - Communication

Question 30: Provide the contents of the last message SENT TO Annie Fao via WhatsApp Application on 5/24/2018.

Manufacturer's Expected Response: Yes I know. I will call you in a few minutes.

WebCode	Response
22YJRM	Yes I know. I will call you in a few minutes.
2PK3JP	Yes I know. I will call you in a few minutes.
2UUKEC	Yes I know. I will call you in a few minutes.
42996J	Yes I know. I will call you in a few minutes.
4CQRKA	Yes I know. I will call you in a few minutes.
4N7HNL	Yes I know. I will call you in a few minutes.
6VXEL8	Yes I know. I will call you in a few minutes.
7W9GAR	Yes I know. I will call you in a few minutes.
7WNX6K	Yes I know. I will call you in a few minutes.
7YP3H6	Yes I know. I will call you in a few minutes.
88MVQY	Yes I know. I will call you in a few minutes.
94JJ86	Yes I know. I will call you in a few minutes.
94W9BG	Yes I know. I will call you in a few minutes.
9UUTMX	Yes I know. I will call you in a few minutes.
A2Q6XK	Yes I know. I will call you in a few minutes.
ATHB7D	Yes I know. I will call you in a few minutes.
B3XPLK	Yes I know. I will call you in a few minutes.
B4U49D	Yes I know. I will call you in a few minutes.
CEB8TH	Yes I know. I will call you in a few minutes.
CW7WPB	Yes I know. I will call you in a few minutes.
D2H6QF	Yes I know. I will call you in a few minutes.
DBKM2J	Yes I know. I will call you in a few minutes.
DPMTFN	"Yes I know."
DR6DZH	Yes I know. I will call you in a few minutes.
EZ2BMK	Yes I know. I will call you in a few minutes.
FA2K8F	Yes I know. I will call you in a few minutes.
FML3XX	Yes I know. I will call you in a few minutes.
FV2JUE	Yes I know. I will call you in a few minutes.
FWCHNM	Yes I know. I will call you in a few minutes.
LVHNTTE	Yes I know. I will call you in a few minutes.
NQGLFN	Yes I know. I will call you in a few minutes.
PBMBAX	Yes I know. I will call you in a few minutes.
PFELHB	Yes I know. I will call you in a few minutes.
Q37ZWW	Yes I know. I will call you in a few minutes.
REWD8D	Yes I know. I will call you in a few minutes.
RWF8X3	Yes I know. I will call you in a few minutes.
TF6KA7	Yes I know. I will call you in a few minutes.

TABLE 1

Question 30 - Communication	
WebCode	Response
UMXFKA	Yes I know. I will call you in a few minutes.
UZMCL8	Yes I know. I will call you in a few minutes.
V3PCKJ	Yes I know. I will call you in a few minutes.
V8MVLH	Yes I know. I will call you in a few minutes.
VFWK22	Yes I know. I will call you in a few minutes.
VNNZQ6	Yes I know. I will call you in a few minutes.
WKJPAV	Yes I know. I will call you in a few minutes.
WMDDTR	Yes I know. I will call you in a few minutes.
WUUUHF	Yes I know. I will call you in a few minutes.
XMPFC6	Yes I know. I will call you in a few minutes.
XMTWCN	Yes I know. I will call you in a few minutes.
XX9QNG	Yeah I am planning on buying that today
Y4U2D7	Yes I know. I will call you in a few minutes.
ZE9HK3	Yes I know. I will call you in a few minutes.
ZNEHVP	Yes I know. I will call in a few minutes.

Consensus Result: Yes I know. I will call you in a few minutes.

Expected Response Explanation:

The content of the messages sent and received using the WhatsApp application is stored in the ChatStorage.sqlite database which can be located at: /Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite

Expected Response Illustration:

Contents of the Last Message Sent to Annie Fao:

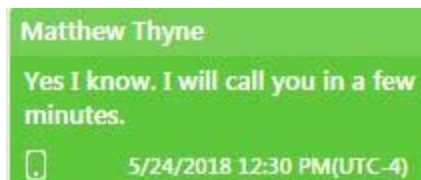


TABLE 1

Question 31 - Communication

Question 31: Provide the contents of the last message RECEIVED FROM Annie Fao via WhatsApp Application on 5/24/2018.

Manufacturer's Expected Response: Your parents should be back soon. We need to do this fast!

WebCode	Response
22YJRM	Your parents should be back soon. We need to do this fast!
2PK3JP	Your parents should be back soon. We need to do this fast!
2UUKEC	Your parents should be back soon. We need to do this fast!
42996J	Your parents should be back soon. We need to do this fast!
4CQRKA	Your parents should be back soon. We need to do this fast!
4N7HNL	Your parents should be back soon. We need to do this fast!
6VXEL8	Your parents should be back soon. We need to do this fast!
7W9GAR	Your parents should be back soon. We need to do this fast!
7WNX6K	Your parents should be back soon. We need to do this fast!
7YP3H6	Your parents should be back soon. we need to do this fast!
88MVQY	Your parents should be back soon. We need to do this fast!
94JJ86	Your parents should be back soon. We need to do this fast!
94W9BG	Your parents should be back soon. We need to do this fast!
9UUTMX	Your parents should be back soon. We need to do this fast!
A2Q6XK	Your parents should be back soon. We need to do this fast!
ATHB7D	Your parents should be back soon. We need to do this fast!
B3XPLK	Your parents should be back soon. We need to do this fast!
B4U49D	Your parents should be back soon. We need to do this fast!
CEB8TH	Your parents should be back soon. We need to do this fast!
CW7WPB	Your parents should be back soon. We need to do this fast!
D2H6QF	Your parents should be back soon. We need to do this fast!
DBKM2J	Your parents should be back soon. We need to do this fast!
DPMTFN	"Your parents should be back soon. We Need to do this first!"
DR6DZH	Your parents should be back soon. We need to do this fast!
EZ2BMK	Your parents should be back soon. We need to do this fast!
FA2K8F	Your parents should be back soon. We need to do this fast!
FML3XX	Your parents should be back soon. We need to do this fast!
FV2JUE	Your parents should be back soon. We need to do this fast!
FWCHNM	Your parents should be back soon. We need to do this fast!
LVHNTE	Your parents should be back soon. We need to do this fast!
NQGLFN	Your parents should be back soon. We need to do this fast!
PBMBAX	Your parents should be back soon. We need to do this fast!
PFELHB	Your parents should be back soon. We need to do this fast!
Q37ZWW	Your parents should be back soon. We need to do this fast!
REWD8D	Your parents should be back soon. We need to do this fast!
RWF8X3	Your parents should be back soon. We need to do this fast!
TF6KA7	Your parents should be back soon. We need to do this fast!

TABLE 1

Question 31 - Communication	
WebCode	Response
UMXFKA	Your parents should be back soon. We need to do this fast!
UZMCL8	Your parents should be back soon. We need to do this fast!
V3PCKJ	Your parents should be back soon. We need to do this fast!
V8MVLH	Your parents should be back soon. We need to do this fast!
VFWK22	Your parents should be back soon. We need to do this fast!
VNNZQ6	Your parents should be back soon. We need to do this fast!
WKJPAV	Your parents should be back soon. We need to do this fast!
WMDDTR	Your parents should be back soon. We need to do this fast!
WUUUHF	Your parents should be back soon. We need to do this fast!
XMPFC6	Your parents should be back soon. We need to do this fast!
XMTWCN	Your parents should be back soon. We need to do this fast!
XX9QNG	Good idea. While you are out, stop by a store and get a rope
Y4U2D7	Your parents should be back soon. We need to do this fast!
ZE9HK3	Your parents should be back soon. We need to do this fast!
ZNEHVP	Your parents should be back soon. We need to do this fast!

Consensus Result: Your parents should be back soon. We need to do this fast!

Expected Response Explanation:

The content of the messages sent and received using the WhatsApp application is stored in the ChatStorage.sqlite database which can be located at: /Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite

Expected Response Illustration:

Contents of the Last Message Received from Annie Fao:

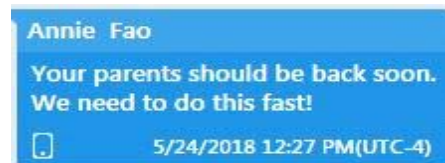


TABLE 1

Question 32 - Communication

Question 32: The user shared their location on 5/24/2018 10:53 AM(UTC-4) using WhatsApp Application. Provide the latitude and longitude of the shared location. Answer using the following format: Longitude: _____, Latitude: _____

Manufacturer's Expected Response: Longitude: -77.396728515625, Latitude: 38.8545341491699

WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
22YJRM	Longitude: 38.854534, Latitude: -77.396729	
2PK3JP	Longitude: 38.854534, Latitude:-77.396729	
2UUKEC	Longitude: 38.854534, Latitude: -77.396729	
42996J	Longitude: 38.854534, Latittude: -77.396729	
4CQRKA	Longitude: 38.854534, Latitude:-77.396729	
4N7HNL	Longitude: 38.854534,Latitude: -77.396729	
6VXEL8	Longitude: -77.396729, Latitude: 38.854534	
7W9GAR	(38.854534, -77.396729)	
7WNX6K	Longitude: -77.396728515625, Latitude: 38.8545341491699	
7YP3H6	Longitude: 38.854838, Latitude:-77.396772	
88MVQY	Longitude:38.854534,Latitude: -77.396729	
94JJ86	Longitude: -77.396729, Latitude: 38.854534	
94W9BG	Longitude: -77.369729, Latitude: 38.854534	
9UUTMX	Longitude: -77.396729, Latitude: 38.854534	
A2Q6XK	Longitude: -77.396729, Latitude: 38.854534	
ATHB7D	Longitude: -77.396729, Latitude: 38.854534	
B3XPLK	Longitude: -77.396729 , Latitude: 38.854534	
B4U49D	Longitude: -77.396729, Latitude: 38.854534	
CEB8TH	Longitude: 38.854534, Latitude: -77.396729	
CW7WPB	Longitude: -77.396729, Latitude: 38.854534	
D2H6QF	Longitude: -77.396728515625, Latitude: 38.8545341491699	
DBKM2J	Longitude: 38.854534, Latitude: 77.396729	
DPMTFN	Longitude: -77.3967590332031 Latitude: 38.854549407959	
DR6DZH	Longitude: 38.854549, Latitude -77.396759	
EZ2BMK	Longitude: -77.396728515625, Latitude: 38.8545341491699	
FA2K8F	Longitude: -77.396729, Latitude: 38.854534	
FML3XX	Longitude: -77.396729, Latitude: 38.854534	
FV2JUE	Longitude: 38.854534, Latitude: -77.396729	
FWCHNM	Longitude: 38.854549, Latitude: -77.396759	
LVHNT	38.854534, -77.396729	
NQGLFN	Longitude: -77.396729, Latitude: 38.854534	
PBMBAX	Longitude: -77.396728515625, Latitude: 38.8545341491699	
PFELHB	Longitude:38.854534,Latitude:-77.396729	
Q37ZWW	Longitude: 38854534, Latitude: 77396729	
REWD8D	Longitude: -77.396729, Latitude: 38.854534	
RWF8X3	Longitude: 38.854534, Latitude: -77.396729	

TABLE 1

Question 32 - Communication		
WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
TF6KA7	Longitude: -77.396729, Latitude: 38.854534	
UMXFKA	Longitude: -77.396729, Latitude: 38.854534	
UZMCL8	Longitude: 38.854534, Latitude: -77.396729	
V3PCKJ	Longitude: -77.396729, Latitude: 38.854534	
V8MVLH	Longitude: -77.396729 , Latitude: 38.854534	
VFWK22	Longitude: 38.854534, Latitude: -77.396729	
VNNZQ6	Longitude: -77.396729, Latitude: 38.854534	
WKJPAV	Longitude: -77.396728515625, Latitude: 38.8545341491699	
WMDDTR	Longitude: -77.396729, Latitude: 38.854534	
WUUUHF	Longitude: -77.396729, Latitude: 38.854534	
XMPFC6	Longitude: 38.854534, Latitude: -77.396729	
XMTWCN	Longitude: -77.396728515625, Latitude: 38.8545341491699	
XX9QNG	-77.396729, 38.854534	
Y4U2D7	Longitude:38.854534,Latitude:-77.396729	
ZE9HK3	Longitude: 38.854534, Latitude: -77.396729	
ZNEHVP	LONGITUDE: -77.396729, LATITUDE: 38.854534	

Consensus Result: Consensus was not achieved for this question primarily because approximately half of the participants labeled GPS coordinates opposite to expected format. These participants reported the expected latitude values as longitude and longitude values as latitude.

Expected Response Explanation:

The GPS coordinates of the location shared via WhatsApp are stored within the ChatStorage.sqlite database which can be located at: /Applications/group.net.whatsapp.Whatsapp.shared/ChatStorage.sqlite

Expected Response Illustration:

GPS Coordinates:

Offset	Length	Value
0x572BD	0x8	Coordinate.Latitude: 38.8545341491699
0x572C5	0x8	Coordinate.Longitude: -77.396728515625
0x58BD8	0x8	Location.TimeStamp: 5/24/2018 10:53 AM(UTC-4)

Timestamp	Position	Category
5/24/2018 10:53 AM(UTC-4)	(38.854534, -77.396729)	WhatsApp

TABLE 1

Question 33 - Media

Question 33: Provide the creation time of the multimedia file named "IMG_0023.MOV". Answer using the time zone set on the device in the following format: Month / Day / Year, Hours: Minutes: Seconds AM / PM.

Manufacturer's Expected Response: 5/21/2018 03:24:54 PM

WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
22YJRM	05/21/2018 3:24:54 PM	
2PK3JP	05/21/ 2018 03:24:54 PM	
2UUKEC	5/21/2018, 3:24:54 PM	
42996J	05 / 21 / 2018, 03:24:54 PM	
4CQRKA	05/21/2018, 3:24:54 PM	
4N7HNL	05/21/2018, 2:24:54 PM(UCT-5)	
6VXEL8	5/21/2018, 3:24:54 PM	
7W9GAR	05/21/2018 02:24 PM	
7WNX6K	05/21/2018 03:24:54 PM	
7YP3H6	05/21/2018 3:24:54 PM	
88MVQY	5/21/2018 3:24:54 PM	
94JJ86	05/21/2018 15:24:54 PM	
94W9BG	05/21/2018, 3:24:54 PM	
9UUTMX	5/21/2018 2:24:54 PM	
A2Q6XK	05/21/2018, 3:24:54 PM	
ATHB7D	05/21/2018, 3:25 PM	
B3XPLK	05/21/2018, 15:25: PM (UTC-04:00)(Plus BST -01:00)	
B4U49D	5/21/2018 3:24:54 PM	
CEB8TH	05/21/2018, 03:24:54 PM	
CW7WPB	5/21/2018 3:24:54 PM	
D2H6QF	05/21/2018, 3:24:54 PM GMT-04:00.	
DBKM2J	5/21/2018 3:24:54 PM	
DPMTFN	05/21/2018 3:24:54 PM	
DR6DZH	05/21/2018 15:24(UTC-4)	
EZ2BMK	05/21/2018: 03:24:54 PM	
FA2K8F	05/21/2018 2:24 PM (UTC-5)	
FML3XX	05/21/2018 03:24:54 PM	
FV2JUE	5/21/2018 19:24:54 PM	
FWCHNM	5/21/2018 03:24:54 PM	
LVHNTTE	05/21/2018, 03:24:54 PM	
NQGLFN	05/21/2018, 3:24:54 PM	
PBMBAX	05/21/2018 15:24:54 PM	
PFELHB	5/21/2018, 03:24:54 PM	
Q37ZWW	05/21/2018, 19:24:00 PM	
REWD8D	05/21/2018 , 3:24:54 PM	
RWF8X3	05/21/2018, 02:24:54 PM	

TABLE 1

Question 33 - Media		
WebCode	Response	** No consensus achieved; Inconsistencies not highlighted **
TF6KA7	05/21/2018, 03:24:54 PM	
UMXFKA	5/21/2018, 3:24:54 PM	
UZMCL8	5/21/2018, 2:24:54 PM	
V3PCKJ	5/21/2018 3:24:54 PM	
V8MVLH	05/21/2018, 03:24:54 PM	
VFWK22	05/21/2018, 03:24:54 PM	
VNNZQ6	5/21/2018 3:24:54 PM	
WKJPAV	05/21/2018, 19:25:07(UTC+0) PM	
WMDDTR	5/21/2018 3:24:54 PM	
WUUUHF	05/21/2018, 03:24:54 PM	
XMPFC6	5/21/2018 2:24:54 PM	
XMTWCN	05/21/2018, 03:24:54 PM(UTC-4)	
XX9QNG	5/21/2018, 3:24:54 PM	
Y4U2D7	5/21/2018, 3:24:54 PM	
ZE9HK3	5/21/2018, 03:24:55 PM	
ZNEHVP	05/21/2018 3:24:54PM (UTC-4)	

Consensus Result: Consensus was not achieved for this question due to answers being reported in various time zones. The answer was requested to be reported in the time zone set on the device (UTC -04:00). The majority of the answers were reported in the requested time zone, however a few participants reported their responses in UTC +00:00 and UTC -05:00.

Expected Response Explanation:

The creation time of "IMG_0023.MOV" can be found within the file metadata. The file can be located at: /var/mobile/Media/DCIM/100APPLE/IMG_0023.MOV

Expected Response Illustration:

Creation Time:

com.apple.quicktime.location.ISO6709	+38.8719-077.2622+096.627/
com.apple.quicktime.software	11.2
com.apple.quicktime.make	Apple
com.apple.quicktime.model	iPhone 6
com.apple.quicktime.creationdate	2018-05-21T15:24:54-0400

TABLE 1

Question 34 - Media

Question 34: What type of file was received from + 1 571-484-0504 on May 23, 2018 at 3:33:23 PM GMT-04:00 via WhatsApp application. Provide the file extension of the file. (Ex: .docx)

Manufacturer's Expected Response: .JPG

WebCode	Response
22YJRM	.JPG
2PK3JP	.jpg
2UUKEC	.jpg
42996J	jpeg
4CQRKA	.jpg
4N7HNL	.jpg
6VXEL8	.jpg
7W9GAR	.jpg
7WNX6K	.jpg
7YP3H6	.jpg
88MVQY	.jpg
94JJ86	.jpg
94W9BG	.jpg
9UUTMX	.jpg
A2Q6XK	jpg
ATHB7D	Ex: .jpg
B3XPLK	.jpg
B4U49D	.jpg
CEB8TH	.jpg
CW7WPB	.jpg
D2H6QF	A colour jpg image file was received, the image shows the back of a males head with a noose around his neck. The man in the image is holding the noose in both of his hands positioned by the side of his neck, with the noose attached to a ceiling fan above his head. The file extension of the image is .jpg
DBKM2J	.Jpg
DPMTFN	.jpg
DR6DZH	.jpg
EZ2BMK	.jpg
FA2K8F	.jpg
FML3XX	.jpg
FV2JUE	.jpeg
FWCHNM	.jpg
LVHNTTE	.jpg
NQGLFN	.jpg
PBMBAX	.jpg
PFELHB	.jpg
Q37ZWW	.jpg
REWD8D	.jpg

TABLE 1

Question 34 - Media	
WebCode	Response
RWF8X3	.jpg
TF6KA7	.jpg
UMXFKA	.jpg
UZMCL8	jpeg
V3PCKJ	.jpg
V8MVLH	.jpg
VFWK22	.jpg
VNNZQ6	.jpg
WKJPAV	.jpg
WMDDTR	.jpg
WUUUHF	.jpg
XMPFC6	JPG
XMTWCN	.jpg
XX9QNG	.jpg
Y4U2D7	.jpg
ZE9HK3	.jpg
ZNEHVP	.JPG

Consensus Result: .JPG

Expected Response Explanation:

The content of the messages sent and received using the WhatsApp application is stored in the ChatStorage.sqlite database which can be located at: /Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite

Expected Response Illustration:

Type of File Received via WhatsApp Application:



TABLE 1

Question 35 - Media

Question 35: What is the make and model of the camera used to capture IMG_0035.JPG? Provide the answer in the following format: Make: _____, Model: _____

Manufacturer's Expected Response: Make: Apple, Model: iPhone6

WebCode	Response
22YJRM	Make: Apple, Model: iPhone 6
2PK3JP	Make:Apple, Model: iPhone 6
2UUKEC	Make: Apple, Model: iPhone 6
42996J	Make: Apple, Model: iPhone 6
4CQRKA	Make: Apple, Model: iPhone 6
4N7HNL	Make: Apple, Model: iPhone 6
6VXEL8	Make: Apple, Model: iPhone 6
7W9GAR	Apple, iPhone 6
7WNX6K	Make: Apple, Model: iPhone 6
7YP3H6	Make: Apple, Model: iPhone 6
88MVQY	Make: Apple, Model: iPhone 6
94JJ86	Make: Apple, Model: iPhone 6
94W9BG	Make:Apple, Model:iPhone 6
9UUTMX	Make: Apple, Model: iPhone 6
A2Q6XK	Make: Apple, Model: iPhone 6
ATHB7D	Make: Apple, Model: iPhone 6
B3XPLK	Make: Apple, Model: iPhone 6 back camera 4.15mm f/2.2
B4U49D	Make: Apple , Model: iPhone 6
CEB8TH	Make: Apple, Model: iPhone6
CW7WPB	Make: Apple, Model: iPhone 6
D2H6QF	Make: Apple, Model: iPhone 6
DBKM2J	Make: Apple, Model: iPhone6
DPMTFN	Make: Apple, Model: iPhone6
DR6DZH	Make: Apple, Model: iPhone 6
EZ2BMK	Make: Apple, Model: iPhone 6
FA2K8F	Make: Apple, Model: iPhone 6
FML3XX	Make: Apple, Model: iPhone 6
FV2JUE	Make: Apple, Model: iPhone 6
FWCHNM	Make: Apple, Model:iPhone 6
LVHNTTE	Apple iPhone 6
NQGLFN	Make: Apple, Model: iPhone 6
PBMBAX	Make: Apple, Model: iPhone 6
PFELHB	Make:Apple, Model:iPhone6
Q37ZWW	Make: Apple, Model: iPhone 6
REWD8D	Make: Apple, Model: iPhone6
RWF8X3	Make: Apple, Model: iPhone 6
TF6KA7	Make: Apple, Model: iPhone 6

TABLE 1

Question 35 - Media	
WebCode	Response
UMXFKA	Make: Apple, Model: iPhone 6
UZMCL8	Make: Apple, Model: Iphone6
V3PCKJ	Make: Apple, Model: iPhone 6
V8MVLH	Apple, iPhone6
VFWK22	Make: Apple, Model: iPhone6
VNNZQ6	Make: Apple, Model: iPhone6
WKJPAV	Make: Apple, Model: iPhone6
WMDDTR	Make: Apple Model: iPhone 6
WUUUHF	Make: Apple, Model: iPhone 6
XMPFC6	Make: Apple, Model: iPhone 6
XMTWCN	Make: Apple, Model: iPhone 6
XX9QNG	Apple, iPhone 6
Y4U2D7	Make: Apple, Model: iPhone6
ZE9HK3	Make: Apple, Model: iPhone 6
ZNEHVP	MAKE:APPLE, MODEL:IPHONE6

Consensus Result: Make: Apple, Model: iPhone6

Expected Response Explanation:

The make and model of the camera used to capture IMG_0035.JPG is stored within the metadata of the image. The image can be located at: /var/mobile/Media/DCIM/100APPLE/IMG_0035.JPG

Expected Response Illustration:

Make and Model of the camera:


Image	Name	Metadata
	IMG_0035.JPG	Camera Make Apple Camera Model iPhone 6 Capture Time 5/24/2018 10:50 AM Pixel resolution 3264x2448

TABLE 1

Question 36 - Media

Question 36: Which web search browser was used to download "IMG_0024.PNG"? Choose one of the following: Chrome, Safari

Manufacturer's Expected Response: Safari

WebCode	Response
22YJRM	Safari
2PK3JP	Safari
2UUKEC	Safari
42996J	Safari
4CQRKA	Safari
4N7HNL	Safari
6VXEL8	Safari
7W9GAR	Safari
7WNX6K	Safari
7YP3H6	Safari
88MVQY	Safari
94JJ86	Safari
94W9BG	Safari
9UUTMX	Safari
A2Q6XK	Safari
ATHB7D	Safari
B3XPLK	Safari
B4U49D	Safari
CEB8TH	Safari
CW7WPB	Safari
D2H6QF	Safari
DBKM2J	Safari
DPMTFN	Safari
DR6DZH	Safari
EZ2BMK	Safari
FA2K8F	Safari
FML3XX	Safari
FV2JUE	Safari
FWCHNM	Safari
LVHNTTE	Safari
NQGLFN	Safari
PBMBAX	Safari
PFELHB	Safari
Q37ZWW	Safari
REWD8D	Safari
RWF8X3	Safari
TF6KA7	Safari

TABLE 1

Question 36 - Media	
WebCode	Response
UMXFKA	Safari
UZMCL8	safari
V3PCKJ	Safari
V8MVLH	Safari
VFWK22	Safari
VNNZQ6	Safari
WKJPAV	Safari
WMDDTR	Safari
WUUUHF	Safari
XMPFC6	Safari
XMTWCN	Safari
XX9QNG	Safari
Y4U2D7	Safari
ZE9HK3	Safari
ZNEHVP	SAFARI


Consensus Result: Safari

Expected Response Explanation:

According to the artifacts found within the image metadata, timeline, and internet search history, the Safari browser was used to capture IMG_0024.PNG

Expected Response Illustration:

Image Creation Date/Time and Timeline Event:

 **IMG_0024.PNG**

Hex View Image view **File Info**

Find:

- General**
- Offsets**
- Date & Time**

Creation time	5/22/2018 03:31 PM(UTC+0)
Modify time	5/22/2018 03:31 PM(UTC+0)

Log Entry Go to

Identifier:	nsurlsessiond/com.apple.mobilesafari
Timestamp:	5/22/2018 11:30 AM(UTC-4)
End Time:	
Application:	com.apple.mobilesafari
Severity:	
Source:	iPhoneNetworkDataUsage

Additional Comments

TABLE 2

WebCode	Additional Comments
22YJRM	The .Tar file included an encrypted backup for which I had not been provided a password. This was guessed as 1234.
B4U49D	Question 36 should be worded differently, the information is consistent with a screenshot being captured from the safari application being open to a specific page not downloaded from safari. Question 33 could be confusing because the creation time of the file UTC-4 and the record time is UTC-5 Overall I appreciate the layout of the test. The questions were good.
CW7WPB	Q36 is formatted incorrectly, I believe. The picture in question is a screenshot taken by the device and is not technically a transfer of a file from one device to another, which is what a download is. I believe it would be more accurate if formatted as; Which web search browser was used to CAPTURE "IMG_0024.PNG"? Choose one of the following: Chrome, Safari (correction in all caps)
UMXFKA	The wording of some of these questions is confusing. Specifically with the questions on incoming and outgoing phone calls. It is also very confusing about format answers should be answered in.
WMDDTR	In reference to question #36: Safari is the browser; however this image is a screenshot taken by the device and not a downloaded image.
ZE9HK3	There is evidence to support the violation of assisted suicide. Several text messages encouraging the victim to proceed with his plans of suicide.
ZNEHVP	This test seems to better in line with a "real" extraction in the forensic world. The questions were more realistic.